Cybersecurity & Boards: Realising Competitive Advantage

Ruchi Goyal

A thesis submitted in partial fulfillment of the requirements of the University of Reading for the degree of Doctor of Philosophy

Henley Business School

University of Reading

June 2023

Declaration

I confirm that this is my own work and the use of all information from other sources has been appropriately acknowledged.

- *Ruchi Goyal*

Acknowledgements

A few years ago, my parents' birthday wish for me was to study more, get another degree, and realise my potential beyond the middle management corporate existence, which had left me discontented. My loving niece, Mishthi, suggested moving to the UK would be a fitting solution to my woes. As I sat contemplating my future path, my wise sister, Rita, pointed me towards a PhD, even though I did not necessarily envision it for myself then. She also introduced me to my distinguished supervisors Professors Nada and Andrew Kakabadse, who are not only extraordinarily wise but inordinately kind as well, and for which I am so thankful. Thus, the seeds for this thesis were germinated.

Just as a seedling needs various other factors to grow into a flourishing plant, I have benefited from the unconditional support of my friends, colleagues, and other generous benefactors along the way. My undergraduate degree course teacher, Professor Raizada, helped me find my voice and literary leanings through Club Literati, and has been invaluable in recommending me for this degree. Similarly, my former boss, Sohan, has been a champion of my desire to expand my horizons by supporting my application. Also, my spiritual *guru*, Sharmaji, has helped me stay true to my inner purpose, and guided me through my life and as an early career academic much before this doctorate came to fruition.

My friends, dotted all over the world and despite the geographical distance, have always encouraged me to embrace my intellectual self. Canduji's consistent advice and vociferous support have helped me to find some answers, and enjoy the process, too. Sumi has been one of my most loyal, reliable, and gentlest friends, providing the metaphoric sunlight for my growth. Megha, my soul sister, despite being the farthest from me, has provided me the symbolic nourishment to carry on irrespective of my circumstances.

Tanya has forever been a pillar of strength for me and continues to inspire me to this day. Archu and Jags have patiently provided me positivity and unrestricted affection. Shweta gently led me into the field of teaching when it was an alien notion for me and, together with Apoorva, helped me appreciate it as a vocation. Sanya has been like my little sister, with wisdom and inner strength beyond her years. Varun's support was vital for me to step into this unknown path, for which I am thankful. Similarly, NJ, Vidhi, and Kawal have offered their consistent support from afar. Başak, Chengcheng, Natalya, Asma, Sasha, Matteo and Nick have been precious with their friendship to me in a new country, and as my fellow PhD warriors. Anni has been a godsend with her patience, positivity, and indefatigable curiosity, for which I am inspired to be a better person.

My colleagues at Henley Business School and the University of Reading have been enormously helpful with their support and facilitation. Prof. James Walker, Prof. Rajneesh Narula and Dr. Joe Lane, in particular, have been incredibly kind by inviting me to join as staff and develop a new relationship with the school, of which I am extremely proud and thankful. They have each been patient and supportive of me, helping me learn, grow, and find my strengths, as I juggled teaching and studying. I am simultaneously thankful to the virtual strangers within the governing corporate bodies in the UK, who supported my research by participating in it.

I consider the Kakabadses to be nothing less than a reward of my good past *karma*. And as extraordinarily brilliant, wise mentors and champions for me, they warrant a second mention. They are the gardeners enabling this plant to grow into a tree that hopes to support others in the future.

My parents have been amazingly patient, loving, and facilitative throughout my entire existence and, especially, through this doctorate journey. My mother, a true embodiment of humility, has forever inspired me to never give up, which has been an invaluable lesson. My father has always supported me, enabling me to witness the pursuit of lifelong learning from close quarters, for which I am forever indebted. This thesis is dedicated to them both.

Abstract

This thesis encompasses a qualitative study which explores the niche field at the confluence of cybersecurity, governing bodies, and corporate strategy. It uses data from 31 in-depth elite interviews with board members and the chief executive team to investigate the way governance of cybersecurity in an organisation can potentially lead to opportunities, including competitive advantage. The thematic analysis has been crucial to unearth findings which contribute to the ever-growing body of knowledge, which is particularly challenging owing to the constantly evolving domain of technology and cybersecurity, as well as the highly private and concealed inner world of boardrooms.

In the 4.0 economy characterised by modern technologies, within the scope of an increasingly cyber-vulnerable virtual realm, further exposed in the wake of the Covid-19 pandemic, this study offers useful insights. The findings highlight the ability of robust cybersecurity practices to enable an organisation to derive opportunities over their competitors. These findings underscore the involvement of governing bodies in the strategic decision-making for cybersecurity, instead of an operational involvement of the IT department to enable robust cybersecurity. The former enables an organisation to achieve advantages over its competitors, as opposed to the latter perspective of several organisations which renders them vulnerable to long-term reputational, financial, and legal damage and/or demise.

Finally, this study urges governing boards, in tandem with their executive teams, to prioritise cybersecurity on their strategic agenda, not only to avoid potential damage but also to exploit opportunities. It contributes to the debate between an operational and strategic perspective to organisational cybersecurity by underscoring the advantages of the strategic stance. The above findings add value to literature which expands the existing discussion of potential sources of competitive advantage to incorporate cybersecurity-led competitive advantages. Simultaneously, reiterating the importance to the practitioner community by highlighting the real-world impact of robust cybersecurity, which is governed strategically, enabling the organisation to derive advantages from it. These findings contribute to the extant literature and field of praxis for this dynamic and fascinating domain.

Contents

Declaration i

Acknowledgements i

Abstract iv

List of Figures xi

List of Tables xii

Abbreviations 0

CHAPTER 1: Introduction 1

1.1 Overview 2

1.2 Research Rationale 2

1.3 Research Scope, Aims, Objectives, and Research Question 3

1.4 Research Contributions 4

1.4.1 Contribution to Theory 4

1.4.2 Contribution to Praxis 6

1.5 Thesis Structure 7

1.6 Chapter Summary 7

CHAPTER 2: Literature Review 9

2.1 Introduction 10

2.2 Boards & Corporate Governance 10

2.2.1 Overview 10

2.2.2 History of Corporate Governance 11

2.2.3 Contribution of Boards 13

2.2.4 Role of Boards 15

2.2.4.1 Main boardroom roles 15

2.2.4.1.1 Support 16

2.2.4.1.2 Control 18

2.2.4.1.3 Maintenance 19

2.2.4.1.5 Linking 20

2.2.4.1.5 Coordinating 21

2.2.4.1.6 Strategic 23

2.2.4.2 History of Stewardship 25

2.2.4.3 Significance of Stewardship today 26

2.2.5 Board Dynamics 28

2.2.5.1 Structural framework 29

2.2.5.2 Inter-relational forces 29
2.2.5.3 Decision-making 30
2.2.6 Summary of Boards & Corporate Governance 30
2.3 Strategising for Competitive Advantage 31
2.3.1 Overview 31
2.3.2 Boards’ Involvement in Corporate Strategy 32
2.3.3 Critical Elements of Strategy 35
2.3.3.1 Mission Development or ‘ends’ 36
2.3.3.2 Resource allocation or ‘means’ 36
2.3.3.3 Strategy formulation or ‘ways’ 37
2.3.4 Strategy Execution 38
2.3.5 Competitive Advantage Unpacked 39
2.3.6 Sources of Competitive Advantage 41
2.3.6.1 Intellectual Capital 43
2.3.6.2 Dynamic Capabilities 44
2.3.6.3 Risk Management 45
2.3.6.4 Combination of IT and ICT/Cybersecurity 47
2.3.7 Summary of Strategising for Competitive Advantage 49
2.4 Cybersecurity 50
2.4.1 Overview 50
2.4.2 Is Cybersecurity an Element of Compliance or Stewardship? 51
2.4.3 Historical View of Cybersecurity 52
2.4.4 Cybersecurity Today 56
2.4.5 Preparing for Cybersecurity Tomorrow 59
2.4.6 Cybersecurity as an implement of Corporate Strategy 64
2.4.7 How Significant is Cybersecurity? 67
2.4.8 Summary of Cybersecurity 69
2.5 Research Gap 69
2.5.1 Research Opportunity 70
2.5.2 Research Question 71
2.6 Theoretical Foundation 71
2.6.1 Considered Theories 71
2.6.1.1 Resource-Based View 72
2.6.1.2 Role Theory 73

2.6.1.3 Agency Theory....75
2.6.1.4 Real Options Theory....76
2.6.1.5 International Relations Theory....77
2.6.1.6 Stakeholder Theory....78
2.6.1.7 Complexity Theory....79
2.6.1.8 Contingency Theory....79
2.6.2 Guiding theory - Stewardship Theory....80
2.7 Chapter Summary....82
CHAPTER 3: Research Methodology....84
3.1 Introduction....85
3.2. Philosophical Position....85
3.2.1 Ontological position....85
3.2.2 Epistemological position....87
3.2.3 Axiological position....88
3.3 Research Design....89
3.3.1 Research Approach....90
3.3.1.1 Narrative approach....90
3.3.1.2 Phenomenological approach....91
3.3.1.3 Ethnographic approach....91
3.3.1.4 Case Study approach....92
3.3.1.5 Qualitative Interview approach....93
3.3.2 Inquiring Logic....94
3.3.2.1 Deductive approach....95
3.3.2.2 Abductive approach....95
3.3.2.3 Retroductive approach....96
3.3.2.4 Inductive approach....96
3.3.3 Research Context....97
3.3.4 Levels of Analysis....98
3.3.5 Unit of Analysis....99
3.3.6 Time Horizon....99
3.3.7 Sample Selection....99
3.3.7.1 Sample specifics....99
3.3.7.2 Methods of sampling....101
3.3.7.2.1 Convenience sampling....101
3.3.7.2.2 Snowball sampling....102

3.3.7.2.3 Quota sampling 102
3.3.7.2.4 Purposive sampling 103
3.3.8 Data Collection Strategy 103
3.3.8.1 Document/material culture...104
3.3.8.2 Focus group...105
3.3.8.3 Observations 105
3.3.8.4 Interview 106
3.3.9 Data Analysis Strategy 107
3.3.9.1 Content analysis...108
3.3.9.2 Document analysis...108
3.3.9.3 Discourse analysis...109
3.3.9.4 Narrative analysis..110
3.3.9.5 Thematic analysis..110
3.3.10 Researcher Involvement...111
3.3.11 Ethical Considerations...112
3.3.11.1 Recording of data..112
3.3.11.2 Maintaining data confidentiality...113
3.3.12 Summary of Research Design 114
3.4 Pilot Study..115
3.4.1 Purpose of the Pilot Study..115
3.4.2 Pilot Study Sample 115
3.4.3 Pilot Study Data Collection..115
3.4.4 Pilot Study Data Analysis...116
3.4.5. Pilot Study Findings 116
3.4.6. Pilot Study Learnings 119
3.5 Research Methods: Main Study 120
3.5.1 Gaining access...120
3.5.2 Main Study Sample 122
3.5.3 Elite Interviewing..124
3.5.4 Data Analysis 125
3.5.4.1 Transcription of Interview Data...126
3.5.4.2 Applying Thematic Analysis 126
3.5.4.3 Researcher Bias..129
3.6 Chapter Summary..130
CHAPTER 4: Data Analysis & Discussion...131

4.1 Introduction 132
4.2 Theme Development 132
4.3 Theme 1: Organisation 134
4.3.1 Organisational Characteristics Impacting CS needs 134
4.3.1.1 CS Perspective of Organisation 135
4.3.1.2 Ethical Point of View 138
4.3.1.3 Organisational features 140
4.3.2 Organisational Decision-makers for CS 143
4.3.2.1 Board characteristics 144
4.3.2.2 Final decision makers for CS 146
4.3.3 Summary of Theme 1 148
4.4 Theme 2: Challenges to Robust CS 148
4.4.1 CS Incidents 149
4.4.2 Macro-economic Challenges 152
4.4.2.1 Pandemic 152
4.4.2.2 Industry-level challenges 154
4.4.2.2.1 People challenge 154
4.4.2.2.2 Tech acceleration challenge 156
4.4.2.2.3 Criminal motivation/access challenge 158
4.4.2.2.4 Big market for CS products challenge 160
4.4.3 Summary of Theme 2 161
4.5 Theme 3: Tools for Confronting CS Challenges 161
4.5.1 Board Engagement Levers 161
4.5.1.1 Risk associated with CS 162
4.5.1.2 Costs associated with CS 164
4.5.1.3 Inhibition around CS 167
4.5.2 Insights 169
4.5.2.1 Correct board language 169
4.5.2.2 People, processes, technology 172
4.5.2.3 Elementary realisations 175
4.5.3 Regulation 176
4.5.4 Summary of Theme 3 180
4.6 Theme 4: Advantages from Robust CS 180
4.6.1 Competitive Advantage from Robust CS 181
4.6.2 Organisation specific advantages from robust CS 184

4.6.2.1 Trust 184

4.6.2.2 Reputation 186

4.6.2.3 Business growth 188

4.6.3 Summary of Theme 4 190

4.7 Winners 190

4.8 Surprising Theoretical Finding 193

4.9 Chapter Summary 194

CHAPTER 5: Conclusion 196

5.1 Introduction 196

5.2 Summary of Findings 197

5.3 Emergent Model - Developing Propositions 203

5.4 Evaluation of Research Quality 211

5.5 Achievement of Research Aims and Objectives 214

5.6 Contributions to Knowledge 218

5.6.1 Contributions to Theory 218

5.6.1.1 Contribution to Resource-Based View 218

5.6.1.2 Contribution to Dynamic Capabilities 221

5.6.2 Contribution to Practice 223

5.7 Research Limitations 226

5.8 Further Research 227

5.9 Personal Reflection 229

5.10 Chapter Summary 231

References 232

Appendix 1: Research Invite Letter (through LinkedIn InMail) 278

Appendix 2: Interview Guide 279

Appendix 3: Sample Interview Transcript 280

Figures

Figure 2.1 Roles of Boards. *16*

Figure 2.2 Evolution of cybersecurity in literature. *54*

Figure 3.1 Coding process. *116*

Figure 3.2 Thematic analysis process. *127*

Figure 5.1 Emergent model from the study. *203*

Tables

Table 3.1 Summary of Research Design. *114*

Table 3.2 Pilot data coding. *117*

Table 3.3 Participant details. *123*

Table 3.4 Industry sector split in participants. *124*

Table 3.5 Stages of theme development. *129*

Table 4.1 Summary of themes. *133*

Table 5.1 Evaluation of research quality. *211*

Table 5.2 Summary of objectives and findings. *214*

Table 5.2 Contribution to Resource-Based View. *217*

Table 5.3 Contribution to Dynamic Capabilities. *220*

Table 5.4 Contribution to practice. *222*

Abbreviations

Abbreviation	**Full Form**
AI	Artificial Intelligence
B2B	Business to Business
B2C	Business to Consumer
CBL	Correct Board Language
CDR	Corporate Digital Responsibility
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CNI	Critical Infrastructure Industry
CS	Cybersecurity
CTO	Chief Technology Officer
HRM	Human Resource Management
FCA	Financial Conduct Authority
FTSE	Financial Times Stock Exchange
GDPR	General Data Protection Regulation
ICT	Information and Communication Technology
IoT	Internet of Things
IT	Information Technology
KPI	Key Performance Indicators
ML	Machine Learning
PPT	People Process Technology
PRA	Prudential Regulation Authority
ROI	Return on Investment
SIRO	Senior Information Risk Officer
virtual CISO	outsourced Chief Information Security Officer
WFH	Work From Home

CHAPTER 1: Introduction

1.1 Overview

This chapter establishes the foundation of the edifice of the thesis. It introduces the idea behind the thesis which seeks to explore the fascinating field of cybersecurity and the manner in which it is incorporated within corporate strategy to realise competitive advantage.

The chapter opens with an explanation of the research rationale behind the thesis leading to the primary question this thesis wishes to respond to, including delineating the research aims and objectives. It further highlights the contributions made by this research to the fields of theory and praxis, followed by a brief account of the thesis structure organised through the subsequent chapters.

1.2 Research Rationale

The 4.0 economy has brought digitalisation to the forefront of contemporary businesses. Several aspects of this digitalisation, such as advanced technologies (like IoT, AI, cloud computing), have been primarily applauded for bringing convenience, autonomy, and augmenting interconnectedness amongst devices. While this has enabled unprecedented growth in certain businesses, simultaneously it has also led to the proliferation of cyber based security concerns as considerable volumes of data are now being stored and maintained in the cyber realm. The ability of cyber incidents to, in some cases, irrevocably alter the course of an organisation’s future performance and survival has brought intense relevance to the field of organisational cybersecurity. It then becomes incumbent upon organisations to safeguard their cyber realms containing stakeholder data and other virtual assets, thereby enabling a competitively safer organisational future.

In such a scenario, it is worth contemplating if, in this evolved and dynamic technological landscape, there may be a possibility to draw a competitive advantage from safeguarding organisational cyber realms, when significant numbers of organisational peers are incapable of rising to the challenge. Is there an opportunity to allow cyber vulnerabilities to be metamorphosed into organisational strengths, by safeguarding the *gold* of the knowledge era - stakeholder data? If so, how may boards, with their executive craft, implement a corporate strategy to incorporate cybersecurity and realise this cybersecurity-led competitive advantage?

Additionally, Covid-19 pandemic has considerably augmented the global challenge, faced by boards of directors alike, to safeguard their cyber realms. Organisations which did not choose to secure their cyber assets have, since, either faced considerable damage to their reputation, legal status, financial performance, or, in certain cases, even organisational demise. Thus, in an unprecedented way, the recent pandemic has heralded board-level involvement in this area, in an attempt to defend their cyber realms (extending it to organisational security). Several organisations, however, have chosen to affect an aggressive stance to defend their cyber realms. Although this study commenced a few months prior to the pandemic, the bulk of the research witnessed the globally evolving aftermath of the pandemic, coupled with the advancement of technologies. Thus, this study not only responds to the researcher's curiosity, but it is also necessitated by macro-economic events that have irrevocably changed the way organisations conduct businesses in the present and future.

Finally, from a theoretical perspective the dialogue surrounding resource-led competitive advantages has existed for the better part of the century. However, in the 4.0 economy, perhaps the nature of this dialogue ought to evolve to incorporate novel sources of competitive advantage that are long-term, dynamic, and offer adequate resilience from which to secure organisation futures. Could we expect a newfound resource, or a collection of resources, to enable this advantage over peers, or develop a capability adequately dynamic to offer long-term opportunities? Thus, in answering these questions, this research has significant connotations to academic literature as well as practical considerations for the industry at large.

1.3 Research Scope, Aims, Objectives, and Research Question

In the contemporary 4.0 economy, digitalisation has brought expansive changes to cybersecurity planning and strategy in organisations. Evidently, some of these organisations are able to manage their cybersecurity more effectively than others. The premise behind this study has been to explore whether cybersecurity *governance*, instead of its *management*, is the differentiating factor. Thus, the aim of this study is to *explore how governing boards incorporate cybersecurity as a critical component of their corporate strategy with the potential to realise a competitive advantage.*

For a subject area as dynamic as technology, and comparatively lower on the historical organisational priority inventory as cybersecurity, research and practitioner reports are equally relatively under-developed. However, with global events such as the Covid-19 pandemic, unprecedented exposure of cyber vulnerabilities and their impact on organisational performance, cybersecurity has swiftly ascended the strategic priority of organisations. In such a scenario, this study is uniquely positioned to explore the evolving cybersecurity landscape of organisations, through the perspective of individuals on their governing bodies. Thus, the following objectives are sought through this research:

i. To explore the extant literature surrounding strategic decision-making on cybersecurity strategy, with a potential possibility of deriving a competitive advantage;
ii. To ascertain precisely how board directors in conjunction with their executives, craft their cybersecurity strategy, through elite interviews with 25-30 such individuals; and
iii. To propose a model explaining the challenges which consequently determine an organisational stance on cybersecurity strategy and implementation, and the path to realising a competitive advantage.

As the chapters ahead explains, the exploration of existing pieces of literature has allowed the following research question to emerge:

'How do board directors consider and position cybersecurity as a critical element of corporate strategy in order to realise competitive advantage?'

1.4 Research Contributions

This research makes contributions to strategic management literature with a specific focus on the theories of the Resource-based View (Wernerfelt, 1984) and Dynamic capabilities (Teece, Pisano and Shuen, 1997). Simultaneously, this study provides meaningful suggestions for organisations and their governance personnel, including the governing board directors and leadership team, with implications for regulations and policy.

The contributions to both these areas are elucidated in Chapter 5, which are summarised below:

1.4.1 Contribution to Theory

The primary theory that this research builds on is the Resource-based View (Wernerfelt, 1984) with a focus on the resources of a firm which allow it to gain and sustain superior performance (Barney and Clark, 2007). With several resources available to an organisation, cybersecurity-led competitive advantage is highlighted through this study. This research is key in underscoring the significance of safeguarding stakeholder information/ data, which enables their trust within the organisation. This enables an upstanding organisational reputation, which functions as a socially complex intangible asset (Rindova, Williamson and Petkova, 2010) and allows the organisation to derive competitive advantage from it.

While honourable reputation (Klein, 1978) and trustworthiness (Barney and Zajac, 1994) have been accepted as valuable intangible assets to an organisation, attaining them through robust cybersecurity mechanisms is highlighted in this study. Robust cybersecurity practices are identified as a form of a collection of small decisions and tacit attributes (Reed and DeFillipi, 1990), which further enable stakeholder trust and uphold organisational reputation. Thus, this research contributes by advancing the perspective on resources, confirming, and extending it to incorporate cybersecurity-led enhancement of stakeholder trust and organisational reputation. Especially in the knowledge era, drawing this association between these three elements helps expand the scope of resources capable of enabling competitive advantage for an organisation.

Furthermore, to the perspective of Resource-based View as propounded by (Mata, Fuerst and Barney, 1995), this research is valuable in confirming and extending the perspective on IT based competitive advantages, while simultaneously illustrating their relevance as an integral component of an organisation's cumulative IT assets. Thus, this study expands the discussion of resources on the one hand, while on the other, drawing an association between cybersecurity and intangible assets including stakeholder trust and reputation, on the path to attaining competitive advantage from it.

The other theory this study builds on is the Dynamic Capability View (Teece, Pisano and Shuen, 1997). This study contributes by confirming and extending the perspective of periods of intense technological change, such as currently identified - where an organisation's ability to uphold stakeholder trust by safeguarding their information within the organisation through robust cybersecurity - may be viewed as a dynamic capability, with the potential to provide a competitive advantage. Realising that the way an organisation chooses to safeguard its stakeholder information is a capability, it is able to build and hone the same over a period of time, instead of merely purchasing a combination of elements, as has been highlighted by this research.

For instance, small cyber breach attempts which did not lead to compromise or those experienced by organisational peers (Ashraf, 2022) enable an organisation to learn from small failures leading to the enhancement of future processes. For cybersecurity, such experiences are valuable in identifying a combination of elements (including personnel, IT assets, cyber insurance, etc.) specific to the organisation, which functions together as a robust cybersecurity mechanism. This is a dynamic capability that the organisation has developed over time, and is specific to the organisation, thereby enabling competitive advantage.

1.4.2 Contribution to Praxis

This research makes worthy contributions to the field of practice not limited to cybersecurity and cyber-defence, but also to the larger organisational landscape in aspects of stakeholder trust, organisational reputation, and competitive advantage. By engaging the governing boards in the decision-making process for cybersecurity, organisations invariably make their priority for cybersecurity explicit to their stakeholders and the external industry at large. Furthermore, this choice also enables them to fortify the protection of their cyber assets, and the valuable information and data they contain. This simple ability to safeguard stakeholder data allows the organisation to benefit from stakeholder trust, which it is able to leverage to garner reputation and function as an effective advantage over its competitors.

This insight to associate the act of safeguarding organisational cyber realm with upholding reputation toward attaining competitive advantage is the outcome from this study. This is of particular value in persuading corporate governance elements - including boards and executive committees - to be strategically involved in cybersecurity decisions in the organisation, instead of assigning them to the IT department. The board involvement, furthermore, enables the organisation to strategise an ordinarily operational matter, to gain several benefits from it (as explained in Chapter 4 and 5). This approach may be characterised as cybersecurity governance - which incorporates strategic focus to matters of cybersecurity, instead of mere cybersecurity management - which relates more to operational aspects of cybersecurity.

In the increasingly digitalised world of the 4.0 economy, where a majority of organisations are increasingly relying on cyber-assets to function, instead of a mere few organisations within the technology sector or e-commerce firms, this study has far-extensive implications for the industry at large. Since regulations are largely crafted and influenced from practice, this study, coupled with the significant role played by regulations in turn (on cybersecurity decisions in organisations), also has potential policy implications.

Overall, this study offers insights to governing boards and their leadership teams as they seek to implement their cybersecurity strategy with a potential to secure advantages over their rivals. Simultaneously this research helps confirm, illustrate, and expand the scope of associated literature concentrating on resources and capabilities appropriate for the knowledge era.

1.5 Thesis Structure

This thesis is partitioned into five chapters, which began with the current introduction. The following chapter 2 executes the monumental task of reviewing the existing literature on the three main aspects of this research- boards and corporate governance of organisations, strategising for competitive advantage, and cybersecurity - which helped clarify the research gap this study sought to fill. To perform this task, the chapter also explains the theoretical foundations over which the study was erected, in the form of primary and secondary theories from literature.

Chapter 3 elucidates the methodological choices apparent in this study. Starting with the philosophical standpoint, the research design and inquiring logic, the chapter then outlines the data collection methodology, strategy, and sample details. Ethical considerations significant for this study, in addition to details and results of the pilot study, are then elaborated on. Finally, the research methods of the main study are described to close the methodology chapter.

The next chapter - Chapter 4 - encompasses both the analysis and discussion of the data collected through the methodology as outlined in chapter 3. This chapter enumerates and elucidates the 5 primary themes which have emerged from the collected data and are of vital importance towards drawing findings from this study. This analysis of the data collected through primary research is simultaneously discussed through the five themes, with support from contemporary literature. This simultaneous analysis and discussion form the bulk of Chapter 4.

Chapter 5 is the concluding chapter comprising of several elements synchronously working together to interlace the previous four chapters together, along with other essential elements. These include presenting the findings through a model that has emerged from the analysis of the collected data from the primary research. Furthermore, the conclusion chapter reiterates the research aim and objectives and inspects their achievements, while also discussing the contributions made by this study. The chapter then examines the study’s validity, followed by a personal reflection of the researcher, thereby drawing the thesis to a conclusion.

1.6 Chapter Summary

This chapter introduces the research while highlighting the significant elements that constitute the thesis. Starting with the research rationale behind this study, this study delineates the scope, aim, and objectives this research sought to achieve, followed by the contributions to the field of literature as well as practice, made by this research. The following chapter performs the vital function of reviewing the extant literature in the fields of governing boards, strategies associated with deriving competitive advantage, and cybersecurity - which function as the three main pillars of this research.

CHAPTER 2: Literature Review

2.1 Introduction

The 4.0 economy relies significantly on digitalised systems, which has intensified in the aftermath of the Covid-19 pandemic (World Economic Forum, 2022). These digitalised systems have potentially improved decision making-processes - with interconnectedness and autonomous decision-making (Kiss, Breda and Muha, 2019) - they have simultaneously augmented risks to businesses in the form of cybersecurity concerns. This chapter reviews extant literature to explore these concerns associated with cybersecurity, the way organisations manage those issues through the involvement of their governing boards, and the path to potentially derive a cybersecurity- led competitive advantage.

The chapter broadly reviews three diverse bodies of literature - the first being the governing board and broader arena of corporate governance in organisations, the second being the vital role of strategy in deriving competitive advantage, and the third being the dynamic and ever-evolving world of cybersecurity. This review then leads a vital examination of the leading and supporting theories which have a significant influence on this research, and to which this study eventually wishes to contribute. Having reviewed the literature then leads to the discovery of the research opportunity and paves the way for the research question, which this study seeks to answer. The chapter then concludes with a brief summary.

The following three subsections – 2.2, 2.3, and 2.4 - highlight and explain the three broad areas which are integral to this research. Examining the current literature in these areas allows for the consequent identification of the research gap and research question for this study.

2.2 Boards & Corporate Governance

Corporate governance as a term has been prominently in use since the 1980s (L’Huillier, 2014) and is widely comprised of the entire ecosystem of private and public institutions, their business practices, and relationships between corporate insiders and investors (OECD, 2004). These corporate insiders are often represented by the governing boards and, as such boards, and corporate governance have often been used synonymously. This section discusses the first significant pillar of this research concerning the governance of corporates.

2.2.1 Overview

Corporate governance is the arena in which the entirety of this research resides. Attempting to understand how boards position cybersecurity within their strategic role of achieving competitive advantage needs to begin with first appreciating the realm of corporate governance.

Any investigation of corporate governance, in turn, would delve into its history and roots, including within the UK. The way the field of corporate governance has led to the evolution of important influences helps set the appropriate tone to understand the functioning and contribution it makes to corporations, further impacting their odds of survival and success.

While discussing the above, the first step is to recognise that governing boards form a crucial component of effective corporate governance (Demb and Neubauer, 2009). This is vital from the perspective of this study to further identify and recognise their role in corporate strategy. To understand governing boards, their functioning - and often fiercely protected inner workings and approaches - take centre-stage before any discussion over strategic involvement takes place. Appreciating the extent of their influence is then achieved through understanding them better – the contribution they make and the roles they perform. This section follows this route to further explore the perspective of boards and their strategic role that leads to identifying sources of potential competitive advantage for the firm.

2.2.2 History of Corporate Governance

"Corporate governance is the process by which corporations are made responsive to the rights and wishes of stakeholders" (Demb and Neubauer, 1992). While it is owing to the enormous share of economic activity in modern economies, the roles of the board of directors, in specific, and corporate governance, in general, are of fundamental importance (Adams, Hermalin and Weisbach, 2010). Hence, governance is a long-standing area of significance for macro-scenarios like economies. Popularly known to have first been brought to attention in the US, it then followed to other parts of the world. Over the course of history, and well into modern literature, academics have been seeking to explain and evaluate the reorientation of corporate governance along Anglo-American lines (Cheffins, 2001). But what was the sequence of events, and how did it first gain significance?

The corporate form has existed for centuries (Hermalin, 2005). The late 19th and early 20th centuries, however, witnessed a growing managerial revolution with a widening gap between ownership and control. Consequently, following World War II, a new phenomenon took hold of the United States – managerial capitalism. Under this, most large enterprises would not have dominant shareholders who could be capable of running checks and balances on the top management (Cheffins, 2015). Corporate management lacked any real responsibility and created potential for abuse (Mason, 1959). Literature and even popular culture are abounded with instances of exploitation and varying levels of fraudulent activities, which together prompted the identification of the need for the management and boards to have more relevant and instrumental roles to play.

While the executives were continuing in their sophisticated hierarchies, the boards were mostly known to be passive, meeting seldom and conducting only their perfunctory duties, as was pointed out in a study conducted in 1968 (Vance, 1968). As such, without meaningful checks from either shareholders or the governing board, agency problems (first anticipated by Adam Smith (Farrar, 1999)) were prominent at this time, and the corporate management was in dire need of corporate governance. This was also followed by corporate scandals and executive misbehaviours of the time, which could be presumed to be the worst part of the managerial capitalism era. ‘Spectator boards’ (Oliver, 2000) were commonplace, which also contributed to growing incidences of shareholder unrest and ownership losses. All the above collectively contributed to an emerging need for corporate governance. Consequently, in the 1970s in the US, and later in the 1990s in the rest of the world, it gained considerable visibility and importance (Cheffins, 2015). Thus, the era significant of corporate governance had dawned.

Since the UK corporate governance system resembles its counterpart in the US (Cheffins, 2001), *‘corporate governance’* followed in the UK as well, but not until the end of 1980s. It first found significance for the idea of Industrial Democracy (Del *et al.*, 2013) which soon after graduated into a concept of wider importance of corporate governance in the early 1990s. Various theories were analysed, and successive codes of practice were propounded. The Cadbury Committee, in 1992, and later Greenbury committee, Hempel committee and Higgs Committees, have all contributed towards setting of regulations for the field of corporate governance in the UK. (Del *et al.*, 2013) Cumulatively they have highlighted the responsibilities of executive directors and independence of the non-executive directors, emphasising on tighter internal financial controls and procedures for reporting. But with advancing times, the world of corporate governance, as we know it, needs to continually evolve.

An interesting point to note is that corporate governance often suggests that a code of rules and procedures be in place to be followed by firms for effective administration. However, each firm - depending on its size, geography, industry, and other factors - affects its perspective of corporate governance and how it chooses to align with it. Willis (2005) in his paper has drawn links between accurate and reliable record-keeping and corporate governance. A further definition of corporate governance, according to him, involves direction, leadership, and accountability, along with systems and processes. A governing board is looked up to for direction that the firm ought to take, through their leadership, while accountability is a tenet of stewardship. Systems and processes are the tools for achieving the above. Thus, the components of corporate governance were identified, and this further influenced the research in the field.

Over the recent decades, financial crises have posed significant challenges as they have demonstrated that managerial actions impact a wide range of people. Thus, since such challenges are partly brought forth due to evolution of interconnectedness, there is perhaps a case for reconceptualising the firm's responsibilities (Parmar *et al.*, 2010). The evolving perspective of corporate governance has led to a distinct set of opportunities and constraints faced by executives today, from those of their counterparts from the managerial capitalism era (Cheffins, 2015). It would, thus, be reasonable to imagine that the whole realm of corporate governance could potentially change, altering the relative powers of various stakeholders involved (Yermack, 2017).

As the world progresses and times change, the purpose that governing boards fulfil - and their contribution - also potentially evolves with them. While elementary aspects of it may remain the same, they invite attention to evaluate the other aspects which support their firms' odds of long-term success. As we progress into the technologically advanced era of tomorrow, relevant new concepts ranging from Internet-of-Things (IoT), Artificial Intelligence (AI) to Neural Networks (NN), have shifted the entire paradigm. Considering industries are increasingly affected by digitalisation, it may be time to consider the importance of strategically moving from *information technology governance* to *business technology governance* (Valentine and Stewart, 2013). In this era, boards that can incorporate these technological changes/trillion-dollar opportunities into specific new business models, strategies and practices would make the most likely success stories (Grove and Clouse, 2017).

2.2.3 Contribution of Boards

While board members vary in form or function – executive or non-executive, unitary or two-tier boards (Souster, 2014) – their contribution is also influenced by the type of their association to a particular organisation. Beyond the immediate understanding of their monitoring (Hung, 1998) and mentoring (Kakabadse *et al.*, 2001) responsibilities, there are a few others which each organisation relies on its board to contribute through. There could be the hiring and firing (Goergen and Renneboog, 2014) of board personnel, ensuring the checks and balances to avoid self-interested behaviour of the executives, as well as securing resources for the firm as the requirements dictate and capabilities of directors allow.

However, their primary contribution is to strategic capacity, which is discussed in detail in 2.2.4.1.6. Interestingly, literature views the board's involvement in strategy from contrasting active and passive schools. The former views it to be actively initiating, implementing, and evaluating strategic decisions (Johnson, Daily and Ellstrand, 1996; Sellevol, Huse and Hansen, 2007), which aligns with this researcher's views as well. This contribution, in turn, is dependent on the board members' set of knowledge and abilities (Hillman and Dalziel, 2003), which has been recognized as an important attribute in the board's strategic task (Minichilli and Hansen, 2007). Among the scholars who view the board's role as setting strategic parameters, the scope of strategic power has been found to be considerable. This is because they fulfil both *gatekeeping* (corporate objective setting) and *confidence-building* (instilling confidence in executive) functions (Stiles, 2001). The debate between their activeness and passivity is age-old, but recent literature is increasingly conscious of the vital role boards play in strategy.

Another crucial component of their contribution to the firm, besides their skill sets, is the combined influence of their particular personalities (Kakabadse *et al.*, 2001). There is also literature to promote the idea that the internal processes of the board play a mediating role in the functioning of the board as a group of interacting individuals (Barroso-castro, Villegas-peri and Dominguez, 2017). Overcoming the limitation of individual directors' rationality through exchanges between them, thereby improving rationality in decision-making, thus reduces the problem of bounded rationality. Promoting complementarity of the individual members' skills and knowledge allows the board to function as a collaborative team (Barroso-castro, Villegas-peri and Dominguez, 2017), thus strengthening their contribution to the organisation.

In order to better contribute to the firm's welfare, there are a few factors that have been found to positively impact the board directors' contributions. For one, the firm's strategic development requires each director to have an in-depth knowledge of the firm, the industry, competitors, customers, and technology (Hillman and Dalziel, 2003). Furthermore, being aware of firm-specific knowledge allows board members to interact in a common language, thereby enhancing the level of strategic discussion (Nahapiet and Ghoshal, 1998). Another factor is the role of the chairman - to be effectively performed - so as to enable the optimal use of each director's skills and knowledge and for it to have a contribution in the strategy-making. The chair needs to be able to create a climate of active participation (Machold et al, 2011) while coordinating, integrating, and developing individual competences within the board (Barroso-castro, Villegas-peri and Dominguez, 2017). Hence, there are multiple factors which ensure that the governing board is primed to perform to its best abilities, in the interest of the organisation and its shareholders. Once these conditions are fulfilled, the quality of board contribution has the potential to differentiate the firm as a success story.

2.2.4 Role of Boards

Conventionally, there are certain roles that all boards - irrespective of size, age range, type of firm and sector of the firm – are supposed to perform. Literature has enjoyed much attention but an agreement over these roles and their classification has always been left wanting (Hendry and Kiel, 2004). Mintzberg (1983) described seven roles: selecting the CEO, exercising direct control during periods of crisis, reviewing managerial decisions and performance, co-opting external influences, establishing control, and raising funds for the organisation, enhancing the organisation's reputation, and giving advice to the organisation.

On the other hand, Zahra, and Pearce, (1990) approached the roles of the board from three elementary dimensions: service, strategy, and control, (which found widespread support within corporate governance literature, even after a decade (Kakabadse *et al.*, 2001)). A few years later, Johnson et al. (1996) introduced their own perspective to the notion of board roles, and they also supported the idea of three roles, albeit slightly different ones: control, service, and resource dependence. Over the course of time, different scholars have reflected the views of their times by arguing separate roles a governing board plays, which are influenced by their individual perspectives as well. These have shaped our understanding of distinct board processes, and a set of roles which could be understood to reveal their most crucial functions.

2.2.4.1 Main boardroom roles

Interestingly, while the roles enumerated by different voices have often overlapped, their explanations and the boundaries of each role may have differed. With such an ambiguous background, a sound perspective was presented by (Judge and Zeithaml, 1992), who proposed the complementarity of two inherent perspectives of board functions: institutional and strategic choice. They noted that boards appeared to be both institutionally responsive and strategically adaptive. Institutional perspective viewed organisational practices to be predicted and explained by examining industry traditions and firm history (Eisenhardt, 1988) - including the inertial effects of founding conditions (Boeker, 1989). The strategic-choice perspective viewed the actions of organisational actors as a response to adapt to environmental forces (Ansoff, 1987), as an explanation for organisational processes and outcomes.

The above two perspectives offered great insights into board involvement and the factors which affected those. These insights helped further develop two sets of factors which influence board-role performance. The first of these two approaches looked at the actions of the board members to adapt to the external environment; thus, could be termed *extrinsic factors*. The second approach observed the evolved socialised and institutionalised processes of function of boards; thus, the *intrinsic factors* (Hung, 1998). Understanding these factors has led to developing theoretical frameworks for the separate roles often played by governing boards. Having redefined the meaning and purview of each role, thus limiting the ambiguity often associated with the field, these roles have found much popularity within mainstream literature. Encompassed within these two perspectives are the following six roles that cover a range of actions expected from governing boards:

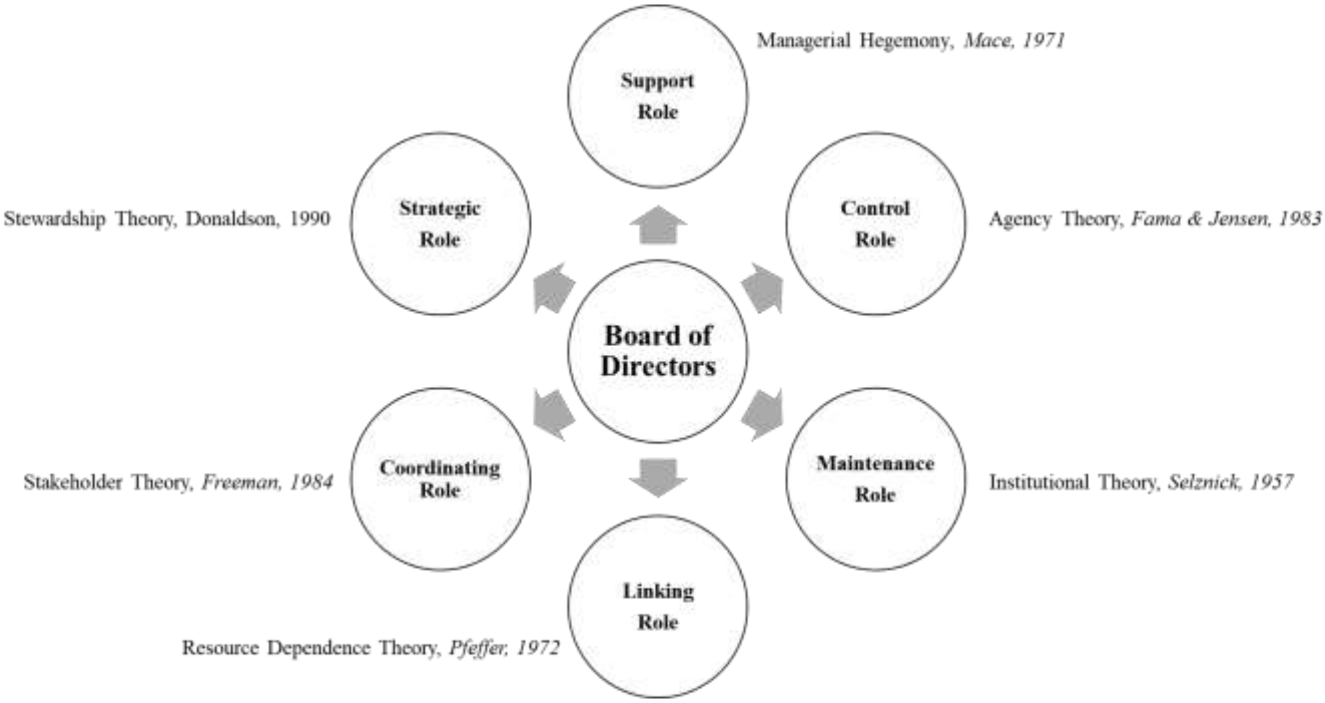
Managerial Hegemony, *Mace, 1971*
Support Role
Stewardship Theory, Donaldson, 1990
Strategic Role
Control Role
Agency Theory, *Fama & Jensen, 1983*
Board of Directors
Stakeholder Theory, *Freeman, 1984*
Coordinating Role
Maintenance Role
Institutional Theory, *Selznick, 1957*
Linking Role
Resource Dependence Theory, *Pfeffer, 1972*

Figure 2.1 Roles of Boards. ***Source****: Adapted from Hung (1998)*

2.2.4.1.1 Support

Governing boards often offer support, especially if the management is the primary body - with powers to influence the chief executive, financial performance, and day-to-day decision-making. Earlier mentioned in the Berle and Means (1932) study, it was later fortified by the work of Mace (1971), who proposed this view through the Managerial Hegemony approach.

Presumed within this view, the governing board only served the limiting role of a "rubber stamp" (Herman, 1981), as the primary strategic choices and organisational decision-making were firmly ensconced in the territory of the management. Proponents of this view envisioned the board with limited powers as they did not exercise control over the executives or the company, leading the shareholders to lose faith in them and thus rendering them ineffective (Stiles, 2001). This theoretical approach highlighted that since the functioning of the organisation was dominated by management, the governing board was relegated to only lending support to the management's operational choices.

Reflecting perhaps views of the time, Mace (1971) explained that boards often declined active roles of decision-making as they were appointed by the management, and as such were subject to managerial discretion. Furthermore, they possessed a relative lack of necessary information/knowledge required to make effective decisions. Scholars insightfully pointed out that since the board was only functioning as a legal entity, it was rendered ineffective in reducing potential agency problems between the ownership (shareholders) and the management (Kosnik, 1987; Mace, 1971; Vance, 1983). This, in addition to the fact that management was sometimes able to reinvest the earnings, reducing the dependence on shareholders for capital (Mizruchi, 1983), did not allow the board much say over the management. Others like Clendenin (1972) supported the notion that, but for times of crisis, boards only conducted superficial reviews, thus reinforcing the notion of operational support.

Further, since management engages in the operational working of the company, they have intimate familiarity of the business - leading to information asymmetry between the board and top management. Also, sometimes the presence of the executives on the governing boards also diluted their authority - leading the management to exercise control (Hendry and Kiel, 2004). Thus, while it could be argued whether boards chose to be not involved or a lack of non-involvement in strategy-making was thrust upon them, their involvement in a supporting role was not viewed as an active one. Nevertheless, this view of the board's role has been the source of much debate and was instrumental in underpinning the passive school of board involvement.

As this research is looking to investigate the board's strategic decision-making process, which influences their stance on cybersecurity, this role of the board may not be an instrumental one. Coming from an acknowledgement of the board's passive engagement in a firm's functioning, the supporting role does not support the premise of this research, which is that a board is actively involved in strategic decision-making. To explore the impact of cybersecurity-related firm’s strategic processes would require a view beyond the management’s role as outlined by the Managerial Hegemony approach discussed above. While important to appreciate the full range of the board’s roles, it may not be important from this study’s point of view. This brings us to the active school of board involvement, which is dominated by the control role.

2.2.4.1.2 Control

Traditionally, control has been viewed as a mechanism to shape the strategic direction of organisations (Stiles, 2001). This is one of the most recognised and popular roles of the board, wherein it supervises the management and protects the interests of the shareholders (Keasey and Wright, 1993), and ascends from the Agency theory, in which Fama and Jensen (1983) propose the governing board’s role to act as a ratifier of the decisions to be implemented, as well as a controller for monitoring the implementation of the decisions made. Essentially taking a less optimistic view of the management, such as it may succumb to individual interests rather than safeguarding those of the shareholders in specific or the firm at large, this theory gained prominence in the late twentieth century.

Popularised further by the Cadbury report (Cadbury Report, 1992), which highlighted the governing functions of the boards as well the need to limit non-executive participation at the board level, this focus supported the view that the management needs to be monitored and controlled to ensure its interests are conforming to those of the company’s. This famous view aligned with the conformance side of the conformance- performance debate (Faludi, 1989) of the 1990s, which argued in favour of the notion of conforming to the motives of the function. While this debate may be returning to the spotlight (Tricket, 1994; Pound, 1995), recent literature has also perceived control beyond the ordinary board constraints over management, rather as a mechanism to shape strategic direction and organisational renewal (Stiles, 2001).

However, there is an argument for firms in uncertain conditions, not faring well under an authoritarian, control-oriented management style (McElwee, 1998), as these would not allow the necessary initiative and strategic stewardship that would help firms respond to a disruptive environment. Mason (2007) observed that in a complex and turbulent external environment, the focus should be on creating an internal environment conducive to co-evolution, which is facilitated by a board exercising its role of monitoring control. He further recommended a form of self-control or ‘self-policing’ which could be understood as a self-organising style of management, in conditions where adapting to and evolving with changes is required. Thus, instead of disregarding this role as archaic, the need is for newer ways to adapt to it in contemporary situations.

From the point of view of this research, the control role promoting the board's strict monitoring of the executive definitely has some influence, though it may not be considered the dominant theoretical framework. Relationships of authority and responsibility (Mitnick, 2019) are elements of this role, and they are consistently useful in overseeing the management. Applied to the context of cybersecurity from a risk-management perspective, the issue of risk compliance is a vital component. Many firms, perhaps not immediately affected by exposure to technology-related risks, follow this practice to ensure their security in the cyber world. Further, the effectiveness of governing boards is often assessed by the control they exercise on the management of the organisation (Hung, 1998), and so the issue of cybersecurity oversight could be potentially viewed from the perspective of this role. The next role discusses the board's limited role in maintenance.

2.2.4.1.3 Maintenance

Organisations subsist on support and legitimacy provided by society which, in turn, require them to follow rules and regulations laid down by them, as was observed by Meyer and Scott (1983). Arising from the social view, this role proposed a somewhat limited range of actions that a board may be able to perform beyond those which it has institutionalised over a period of time. This role was supported by the notion that since organisational structures and processes come to be taken for granted as a consequence of the institutionalisation process (Meyer and Rowan, 1977; Selznick, 1949, 1957; Zucker, 1987), their involvement was limited to maintenance. Supported primarily by the Institutional theory (Selznick, 1957), this role highlighted the pressure faced by organisations and their boards from the external environment which, in turn, socially constrained them to follow taken-for-granted conventions and practices (Ingram and Simons, 1995).

The construct of *isomorphism*, whereby organisations conform to the accepted norms of their populations (DiMaggio and Powell, 1983; Rowan, 1982), weighed heavily on influencing opinions about this role. Another influence for institutionalisation was the way certain firms resisted external pressures by adopting the firm's practices from the time of founding and carrying them through for the rest of the organisation's life (Stinchcombe, 1965). Further, Selznick (1957) argued in favour of institutionalisation by instilling values which promoted the stability and continuity of organisational structure over time. The reason this institutionalisation was considered sensible was perhaps because it pleases external constituencies, portrays a responsible management, and avoids the potential claims of negligence if something goes wrong (Eisenhardt, 1988). This offers great insight, especially in the current circumstances where exposure to legal action could be considered a growing cause of concern for companies.

Drazin and Van de Ven (1985) pointed out that, over time, several internal coordination and control practices tend to get institutionalised, which may affect how they respond to external environments and pressures. Having identified this perspective of the role of the boards, it is helpful to note that in the case of contingent factors, or even changes brought on by advancements such as technology, this role may not allow the board or the firm to be responsive. This is another role from the passive school of board involvement views, which also included the support role. As such, in direct contrast are the roles from the active school, which gain prominence when discussing functions especially pertaining to strategy-making, accessing external resources, and adjusting to environmental factors like technological advancements.

From the perspective of this study, this role is not significant for this research, as it is aimed at appreciating the board's involvement with respect to cybersecurity. As such, the active perspective of the governing board's contribution is presupposed as a factor influencing their choices with regard to managing cyber-related operational decisions. If the board only performs a limited role through maintenance, its valued contribution to strategy would not be possible - which is the premise for this study. Hence, while it is important to note all of the board's various roles, it is also crucial to note which are vital from this research's perspective. The next role discusses the governing board's part in helping a firm secure access to the resources it requires.

2.2.4.1.5 Linking

Since organisations are not self-sufficient and rely on their external environment, their boards perform a crucial role of linking them to the external resources. This linking role has been highlighted in the Resource Dependence theory by Pfeffer and Salancik (1978). It is interesting to note that board of directors often comprises of members of boards of more than one firm, and in this way play enhanced roles in linking the performance, finances, and other resources for employment by each of those organisations. While this *interlock* is used to co-opt threats and uncertainties to their advantage (Useem, 1978), it could also be used to manipulate the available resources of one organisation for another. This presents a great insight on how board members, especially outside directors, prove their usefulness to the organisations on whose governing boards they serve.

Another fascinating perspective of this function is the class solidarity that is brought to the fore. Since board directors could be considered to be unified by their capitalist interests, they often cultivate relationships with each other (Hung, 1998). Such a network of interdependent relationships could even be construed as a coalition, which can exert pressure when needed on the state to safeguard their class interests (Mizruchi, 1983). The directors, through interlocking directorate (Palmer, 1983), often communicate valuable information about their industry sectors (Pennings, 1980), thus offering great links to the firms connected in the said network. However, since these links to access resources are also part of the resources versus power trade-off (Garg and Eisenhardt, 2017), there are instances when directors refuse valuable resources to avoid relinquishing power (Katila et al., 2008; Wasserman, 2006), which renders their linking role defunct in newer firms.

From the perspective of this study, exploring the board's role in crafting a strategy for cybersecurity, this role is limited. In the context of the 4.0 economy, product-use data (the digitalised product created (Schroeder *et al.*, 2019) through modern technology) has been identified as a shared network resource (Lavie, 2006). In such a scenario, the scope of the directors' linking role is expanded; yet it does not throw light on the strategic aspects of how they manage and protect the vulnerabilities of this resource. The resource dependence theory (Pfeffer and Salancik, 1978) views the ways a firm needs to control its external resources. Instead, for this study, the need is to explore the resource-based view (Wernerfelt, 1984) which helps firms strategise for competitive advantage, which may be a useful perspective for issues like cybersecurity. The linking role requires the board members to coordinate their influence on their organisations' advantage, which brings to attention another key role that the boards fulfil – coordinating.

2.2.4.1.5 Coordinating

While the Agency theory viewed two primary parties whose interests are at stake in any given firm – the principal and the agent, the Stakeholder theory introduced by Freeman (1984), threw light on all the interested parties involved in the welfare of the firm. He suggested that in any given firm, there are more than two parties whose interests are at stake; thus, there are many groups in the society (besides owners and employees) to whom the corporation is responsible (Hung, 1998). In this pluralistic approach, a *stakeholder* was identified as *"any group or* *individual who can affect, or is affected by, the achievement of a corporation's purpose"* (Freeman, 1984, pp.46). The inherent idea being that the corporation is responsible to all of its stakeholders and thus needs to coordinate, balance, negotiate, and compromise their interests towards the larger interests of the organisation.

It might be relevant to observe that the stakeholders is a broad term which may encompass various parties whose interests the firm may be responsible to uphold. However, literature has highlighted various ways to categorise the significance of these stakeholders, a popular way is by being identified as *primary* or *secondary*. This is an essential distinction between groups of stakeholders depending on their claims, relationship, and power- dependence (Mitchell, Agle and Wood, 1997) in the firm. An individual or group's stake in an organisation would allow clarity with respect to influence on the firm (Brenner, 1993), thus allowing to differentiate between their importance to it. Another characteristic feature pointed out was their relationship which could be latent (in cases when they are involuntarily or unwillingly placed at risk (Clarkson, 1995)) or actual (stakeholders who influence or are influenced by the organisation (Starik, 1995)). Another distinction could be observed from their power over or dependence on the organisation itself; whether the organisation depends on the stakeholders for its survival, or the stakeholders depend on the organisation for furthering their interests, or for mutually dependent relationships (Mitchell, Agle and Wood, 1997). This identification of stakeholders with respect to their specific association with the firm, could be considered to further influence the coordinating role of the board.

Interestingly, this stakeholder perspective went a step beyond the Resource Dependence theory (Pfeffer and Salancik, 1978) by addressing an important query thrown by it – how should the resources of the firms be managed towards gaining competitive advantage (Priem and Butler, 2001). Thus, coordinating as a function of the governing boards, essentially, gives direction to the resource allocation of the firm, towards different stakeholders (with potentially divergent interests) as well as those of the firm itself. With certain other perspectives of a board's role, the notion of capitalism was supported through business, which made it rather simplistic to skip the idea of being ethically responsible. Some scholars supportive of this view, put forth their hopes on this approach for the potential of bringing ethics back to the centre of the business (Parmar *et al.*, 2010). Thus, this view allowed the board to facilitate a more responsible outlook of the firm through their role, which coordinates between the various stakeholders.

It would be helpful to note that this is the role through which initiatives of the firm largely under the realm of Corporate Social Responsibility (CSR), are brought to light. Adhering to the social obligations of the business (Davis, 1973; Frederick, 1994) was also another essential element of the governing board's role. Goodpaster (1991) added another dimension to this view by bifurcating stakeholders into two types – moral and strategic ones. The former allowed for a bi-directional view where both the firm as well the stakeholders' interests were important and thus needed to be balanced. Opposed to this was the strategic stakeholder whose interests needed to be managed or dealt with, with a unidirectional approach (Frooman, 1999).

The Stakeholder theory's (Freeman, 1984) influence in deciding a board's role in coordinating between the interests of its various stakeholders is an important aspect while exploring how it decides its approach to cybersecurity. A governing board immune to its relationships with vendors, employees, and clients, would not be able to effectively employ a robust strategic plan with respect to cybersecurity. As is later explained, cybersecurity concerns are sometimes fuelled by a firm's risk appetite (Leech and Hanlon, 2017) which, in turn, covers its exposure of risks to both internal (employees) and external stakeholders (customers) alike. Thus, viewing the firm's relationships, besides those to the owners (shareholders) and management, is key to this research which is looking to investigate the board's strategic role. This brings us to the next role performed by governing boards – strategic (Hendry and Kiel, 2004; Nadler, 2004; Hendry, Kiel, and Nicholson, 2010).

2.2.4.1.6 Strategic

Contrasting Cadbury's views of the control function or conformance, Hilmer 1993), opined that the function of boards was to ensure that management was driven towards continuous and effective performance. However, recent literature points to a shift in perspective wherein instead of being in contrast to the Agency theory, modern scholars consider the Stewardship theory to complement the overall view of the governing boards (Shen, 2003; Sundaramurthy and Lewis, 2003). Both these theories had two points in common. One, they both focused on the behaviour of the 'manager' – the member of the supervisory board – and their relation to the executive of the company. And two, they described the notion of the model manager (Glinkowska and Kaczmarek, 2015) – one who furthers his interests, or the other who furthers his interests by advancing those of the firm. This view recognised the range of non-financial motives for executive behaviour, wherein the strategic role contributes towards the larger objective of company stewardship (Hung, 1998;Stiles, 2001).

Bower (1970), Burgleman (1983) and Mintzberg (1983), came to conclude that strategy development in a firm happens at the business unit level. Certain authors like Andrews (1981) opined that governing boards were limited by their role of reviewing strategies formulated by the management, or that boards inadvertently influence strategy-making decisions without realizing their involvement (Henke, 1986). However, such views of the boards' involvement in strategy-making have been limited in expression as well as in popularity. Yet, many of them also agreed that the board set the strategic parameters within which the strategic activity was conducted (Stiles, 2001). Muth and Donaldson (1998) even argue that the insider-dominated boards contribute towards a depth of knowledge, expertise, and commitment, which further facilitates an active strategy role. Thus, the governing board's involvement in running the organisation and having the power to affect the shape and direction of the company (Stiles, 2001) has increasingly been acknowledged and accepted as an integral role.

Scholars like Lynch (1979) have proposed the notion that active and participating boards' lead to management working towards analysing and articulating their plans better. There definitely is a need for more research to further understand the processes which lead to boards being able to perform their strategic role immaculately. However, the above notion is a powerful insight as it not only clarifies the chain of significance but also highlights the desired traits of a governing board - so as to benefit from an efficient and effective management team. Hence, the importance of this role cannot be diminished; in contrast, it needs further exploration to better understand the sophisticated and otherwise private workings of a boardroom. For the purpose of this research the importance of this role, and in turn of this theory, may be considered considerable.

With respect to the objective of this research, the Stewardship theory (Donaldson, 1990), and, in turn, its promotion of the governing board's strategic role underscores the most important of board's roles. This study wishes to explore the motivations for a board choosing its strategic stance on cybersecurity and making those choices more fruitful. As such, just like this role, the board's involvement in strategy and its various components helps explore this framework and offers potential solutions for managing it better in future. As an influence, this role as well as Stewardship theory (Donaldson, 1990) and its other components function as a potentially solid foundation for this research.

2.2.4.2 History of Stewardship

As long as the ownership has existed, stewards were needed to safeguard their interests. The concept of stewardship can be understood to have been around for millennia. Historically, the first crop cultivation and livestock domestication dates back to circa 8000-3000 BC in the Middle East (Miller and Oldroyd, 2018). A settled agricultural society meant the existence of property in the form of land and surplus, which led to differential levels of ownership and reckoning technologies to track economic exchanges and enforce obligation (Oldroyd and Miller, 2011). Accounting, trading, and stewardship were bases which covered an evolutionary society, which may be presumed to have led to the foundation of an early capitalist society.

However, modern usage of the term as well origins of the theory could be traced to human relations school of management theories. McGregor in 1960 presented two contrasting approaches of managerial behaviour – Theory X, which presented the manager as a rational being interested in furthering his own interests, and Theory Y, which saw him as somebody who would be motivated by the satisfaction of a job well done. Such motivation followed that such a manager and the supervisory existed on a relationship of trust, and the organisation's welfare and interests were safeguarded by the manager's pro-organisation behaviour (Glinkowska and Kaczmarek, 2015). Thus, the notion of such a manager acting as a steward for the shareholders' interests was rooted in organisational psychology and sociology, from which originated the Stewardship theory.

Since it finds its roots in the psychological and sociological bases of human behaviour, it accepted that intrinsic motivation and collectivism explained the steward's behaviour (Puyvelde et al., 2012). Should Maslow's pyramid be considered, the psychological factor or the motivation for the steward arises from his higher needs – self-realisation, recognition, achievement, and respect (Davis, Schoorman and Donaldson, 1997). Thus, guided by their internal motivation to fulfil their mission, they do not fall prey to the otherwise popular notion of principal-agent conflict as highlighted in the Agency theory (Caers et al., 2006). Thus, acting for the interests of the entire range of stakeholders, their primary motive is to ensure efficient utilisation of the resources they have been entrusted with (McCuddy and Pirie, 2007). Furthermore, in being effective stewards of the company, the directors are also effectively managing their own careers (Fama, 1980).

Furthering the pro-organisation motives of the steward, Donaldson, and Davis (1991) argued the notion of *CEO duality* wherein the CEO, who is the chair of the governing board, would have the power to determine the strategy for the organisation without the fear of being revoked by an external chairman. While some observers like Michael Jensen (1993) have urged for banning such an event, many others, especially recent scholars, have pointed out the benefit that a combination of titles can potentially bring. The impact on the power dynamics at play when an individual holds two titles, and therefore comparatively more influence over the board and its decisions, becomes especially important during events of CEO succession (Shen and Canella, 2002).

This concept also brought focus to the other aspect of the stewardship – strategic role (Hung, 1998) - which went beyond the limited confines of advising and supervising, which a governing board is ordinarily associated with. Thus, this theory's view of stewardship encompassed service and supervisory roles, but also significantly, a strategic role. While traditional studies viewed boards with a somewhat limited involvement on a firm's strategic direction (Rindova, 1999; Zahra, 1990; Whisler, 1984, Mace, 1971; Lorsch, 1989), recent literature is gradually embracing the key role played by boards in the organisation's strategic tasks and direction (Nadler, 2004; Hendry, Kiel, and Nicholson, 2010). This is another key factor why, in the present and the potential future, the significance of the board's stewardship role may not be diminished.

2.2.4.3 Significance of Stewardship today

For most of the recent corporate governance study history, the majority of the debate has been between Agency and Stewardship, Conformance and Performance (Hung, 1998), Control and Strategy, Conflict and Consensus, outside and inside directors (Forbes and Milliken, 1999; Stiles, 2001; Sison and Kleiner, 2001; Carpenter and Westphal, 2001; Lorsch and Palepu, 2002), and Compliance and Stewardship. All these terms reflect the initial and more popular approach to view these theories as contrasting and at the opposite ends of the spectrum. However, many scholars have advocated viewing and using them in conjunction with each other for best results. This confirms the dominance still assumed by the mentoring aspect of stewardship (Kakabadse *et al.*, 2001), even while it is being shared with the monitoring duties of the agency perspective. However, this in no means demonstrates the lack of ability of stewardship to find significance on its own.

In terms of organisations and regions where it has found support, there are studies which have witnessed the preference for the stewardship concept. While public administration has shown a continuum between agency and stewardship (Schillemans and Bjurstrøm, 2019), stewardship has found more acceptance in corporate governance in Europe and Japan (Glinkowska and Kaczmarek, 2015), and Australian chairpersons perceived themselves as stewards for the enterprise's future vision (Kakabadse and Kakabadse, 2007). We thus understand the significance bestowed on stewardship in non-public sector organisations, within regions like Australia, Europe, and certain countries in Asia. This does not reflect negatively for stewardship on organisations and regions outside the ones mentioned above; rather, it shows the level of acceptance that is already acknowledged. There might still be undocumented evidence of prevalence for this concept, which needs further investigation and empirical support. These are other considerations which shed light on the acceptance and prevalence of stewardship today.

An important multi-method study conducted in UK companies through interviews with board directors, surveys and case-studies drew remarkably interesting insights on the workings of governing boards. (Stiles, 2001) concluded that board involvement in strategy is a primary role, even though companies may not follow a strictly top-down approach for strategy-making. It also highlighted the multi-function nature of board activity, while pointing out that directors mostly insisted on their stewardship duties and wanted to be seen as great professionals who performed their duties well. These directors and their stewardship commitment, comprising of the human capital, led to the value creation process for businesses (Snell and Dean, 1992) - further creating the source of the firm's competitive advantage. This is a great learning, especially with respect to this study which draws on the board's involvement with setting the firm's competitive benefits, as an element of the stewardship aspect.

An area of interest could be - who is associated with stewardship duties within a particular company? While in some organisations, it could be the board directors - or others where the executive or management team shoulders the responsibility along with the board, or even for specific issues - a committee could be created to look after, as stewards. In many cases, the board chairpersons are responsible for stewarding boardroom affairs, including duties like ensuring adequate information flow to NEDs, auditing firm affairs, and determining compensation-related structures (Cadbury, 1992). Deciding the 'who' of stewardship may be subjective for each firm whereby one category, or more than one, plays the role of steward. What is undisputed, though, is that being effective stewards also helps them further their own careers (Fama, 1980), as they recognise the impact of firm performance on the perception of their individual performance (Daily, Dalton and Jr., 2003), motivating them to be good stewards. This aspect of stewardship is neither region nor time specific as it relates to the psychology of the individuals.

Another vital constituent of corporate governance is accountability and unlike agency theory (Fama and Jensen, 1983) - where reliance on stewards is lacking - stewardship theory (Donaldson, 1990) takes a unique perspective. The Berle-Dodd debate (Macintosh, 1999) brought to fore the concept of accountability in financial reporting, moving the objective from stewardship to public interest (Watts and Zimmerman, 1979). Promoting a sense of accountability as a form of following responsibility and adhering to the company's values (Keay, 2017) is simpler because an aura of trustworthiness already exists and, hence, governance measures are strengthened. While it became a part of regulation, stewardship has continued to affect accountability aspects and vice versa. Hence, even from the financial reporting perspective, stewardship remains in focus, as is evident from the UK Stewardship Code 2020 (Stuart, 2019), annually published by the Financial Reporting Council (Council, 2018), highlighting the framework for effective stewardship.

In many organisations today, CEO duality (Donaldson and Davis, 1991) is a common occurrence, which further is an example of stewardship. The stewardship perspective promoted the idea of a common individual who would be head of the executive as well as the governing board, facilitating a unified leadership (Yar Hamidi, 2016) as along with flexible resources for contingencies. Furthermore, today - when technology and networks are the foundation of many a business - the management of IT infrastructure and cybersecurity risk-management are no longer issues for risk compliance, but increasingly a topic of stewardship. Under this, elementary areas such as those discussed above would receive adequate significance, which would lead to intact company reputations and successful enterprises. In such respects, the need for stewardship could be considered to have never been more significant than today.

2.2.5 Board Dynamics

There is extensive literature that has explored the various board processes, behaviour, and inter-relationships to emphasise the importance of board dynamics. After having discussed the contribution and role of the governing boards in the previous sections, it is vital to next discuss the significance of board dynamics on its strategy-making activities. The board dynamics are often elementary to how a governing board may prioritise cybersecurity or choose not to (Gale, Bongiovanni and Slapnicar, 2022), and what may have an influence on technology-related strategic outcomes. Furthermore, exploring governing board members' strategy-making activities requires them to first appreciate how they use their discretion and influence to consider and position strategies for their companies.

Board dynamics may be considered an area encompassing all behaviours and processes involving board directors and their interactions amongst each other. However, there could be certain elements which are considered elementary to board dynamics. Adapted from Van Ees, Gabrielsson and Huse 2009) these could be:

2.2.5.1 Structural framework

The essential formal structure of the board deals with the element of command and control that the board exerts. Drawing from the Agency theory (Jensen and Meckling, 1976) perspective, this would argue rational and opportunistic behaviour on the parts of the agent and principal. The aspect of drawing out an incentive-and-control structure is further influenced by the impact of board dynamics like CEO duality, board composition and board independence on firm performance (Rhodes, Rechner and Sundaramurthy, 2001; Ellstrand, Tihanyi and Johnson, 2002; Randoy and Nielsen, 2002).

For a skill-reliant element of their strategy such as this, the directors may not be able to monitor or advise if they lack the essential relevant information or experience themselves (Carpenter, 2016). Thus, how they approach the subject of technology, keeping it updated, protecting their cyber-realm, and the sturdiness of their technology policy are, in turn, impacted by other elements of board structure.

2.2.5.2 Inter-relational forces

Inter-relationships within the board members are crucial towards their functioning and impact on decision-making. Ordinarily, it would be reasonable to imagine one of the two possible outcomes – coordination or conflict (Van Ees, Gabrielsson and Huse, 2009). In cases where the board members are in conflict with each other, even the chairpersons have been found unable to transform the tensions among members into synergies (Kakabadse, Kakabadse and Barratt, 2006), to manage the boardroom dynamics. Thus, CEO characteristics, social ties, demographic similarity, and the timing of directors' appointments (Finkelstein and D'Aveni, 1994; Westphal and Zajac, 1995; Westphal and Stern, 2006), are all important influences. Further, the social network embeddedness perspectives on organisational behaviour (Granovetter, 1992; Weick, 1995) outline that crucial impact of the information spread through social-structure relations, thus supporting this board dynamic.

Literature has supported views that organisational behaviour is impacted by the social context; social context itself is further moderated by the strategic context (Carpenter, 2016). Boards of companies reliant on technology, favour younger directors with contemporary technological expertise over older directors with prestigious appointments (Kotz, 1998). Thus, it could be understood that boards in such environments, characterised by growth and product differentiation, may also enjoy higher levels of discretion (Hambrick and Abrahamson, 1995), thereby further influencing how they consider and strategise on technology-related decisions.

2.2.5.3 Decision-making

Boards deciding their overall technology strategy have either their cognition or competence (Van Ees, Gabrielsson and Huse, 2009) to rely on. They look to the director competency, experience and knowledge for board functioning and making effective strategic decisions (Westphal and Fredrickson, 2001; Kula and Tatoglu, 2006). Other factors could be cognition and behavioural dynamics, as argued by (Forbes and Milliken, 1999; Rindova, 1999). Together they play a significant role in influencing how the board and leadership make strategic decisions for the company.

Considering firms within the technology industry or even those for which technology is a crucial element of business (which would include most firms in the contemporary 4.0 economy), boardroom dynamics come into special focus. Members of such boards need to exhibit knowledge and skills far above the ordinary requirements of board service (Kotz, 1998). Hence, to examine the elements influencing cybersecurity strategy at a firm, the expertise and relevant experience of the board members becomes vital. Whether they have been *digital natives* (Thomas, 2011) or only adapted to the digitisation in the recent times, their experience in management or as other firm's board members guides their skill set. This further influences the counsel they provide and the strength of their influence on technology-related boardroom decisions.

2.2.6 Summary of Boards & Corporate Governance

In the digitalisation of the current knowledge era (Uhl-Bien, Marion and McKelvey, 2007) the technological ramifications have shaken corporates to their core (Cordes and Stacey, 2017). In light of such advancements, the significance of corporate governance in contemporary times cannot be overstated. Within this context, boards are perhaps progressively being identified as the most crucial component. In such a scenario, the responsibility then lies with them through the strategies they formulate. The board, in conjunction with the top management team, performs its many roles to perfection so as to allow its firm’s survivability into the future. (Zahra, 1990) notes the significance of the above as, together, they need to anticipate the firm’s environment and develop policies to ensure the firm’s survival as well as effective performance over the long-term.

With the changing times, the need for the board’s involvement cannot be overlooked. Its contribution towards the strategising process is instrumental in deciding the organisation’s odds of success relative to its competitors and rivals. ‘Best practices’ in the contemporary world may refer to the appropriate amount of strategic level that the board chooses for itself, and further deciding the role it intends to play in strategy (Oliver, 2000). Thus, corporate strategy is key towards addressing unexpected or even unprecedented events such as cybersecurity threats and pandemics. Furthermore, a board-devised plan allows the firm to choose and craft its strategy for achieving competitive advantage.

2.3 Strategising for Competitive Advantage

Competitive Advantage is a popular concept within strategic management, yet it is widely debated with respect to its meaning and how it may be derived (Peteraf, 1993; Powell, 2001; Ma, 2006; Wang, 2014). The following section explores the strategic involvement towards the attainment of competitive advantage for an organisation.

2.3.1 Overview

Competitive advantage, as a way to both survive and succeed, has been an elementary component of strategy and strategic management since its earliest days. Some may even say that the entire idea of crafting a business strategy is with the end-goal of achieving sustainable competitive advantage. But before delving further into the construct of competitive advantage, what it entails and the various tools required to implement it, the need is to first appreciate the process of strategy-making, and how different boards arrive at deciding their corporate strategies. Is there a universally applicable algorithm, depending upon certain characteristic features, or is it subjective to each firm? Extending Filatotchev, Toms and Wright’s (2006) rejection of the notion of universal corporate governance parameters, even the corporate strategies will need to be linked to the requirements of the firm they are being crafted for. Further, once the strategy has been formulated, what are the essential elements of such a strategic plan? Has this evolved over time and changed in today’s scenario? This understanding goes a long way to appreciate how firms identify sources of potential competitive advantage.

The meaning of competitive advantage, and how it offers potential benefits over the rivals, unlocks the potential for firms to find long-term success in an otherwise dynamic market scenario. As such, a firm's overall corporate strategy, in general, and competitive advantage, in particular, is constantly threatened by both internal and external factors, which could even take the form of radical discontinuity in an extreme scenario (Ghezzi, 2013) from a disruptive environment. But perhaps another perspective to the idea of competitive advantage can help better manage and respond to internal and external environment threats? Competitive advantage often comes equipped with certain options, which organisations can choose as per their respective fit, and hope to thrive and not just survive. Further, while strategising has traditionally been associated with governing boards and top management teams, certain modern literature is also urging for the organisation at a larger scale to be involved (adoption) in the strategy-making process for increasing the chances of the organisation's success.

2.3.2 Boards' Involvement in Corporate Strategy

Board rooms, despite the ample literature that has delved into them, have managed to remain a source of much debate owing to their private functioning and decision-making behind doors, otherwise protected from the public. Since the last century, increasing efforts have been made to allow academic knowledge as well as practitioner accounts to reveal the 'black box of boards' (Pettigrew, 1992) of their inner workings; yet what influences are at play, and how they differ for different firms, still manage to evade public knowledge. The most significant path-breaking activity for a firm that could be considered is its strategic planning, and boards - often with help from their management - conduct this function to varying degrees of success, and sometimes failure. At other times, despite the strategy formulation, companies have faltered and fallen monumentally in the public eye. Is the board to be blamed, or is their strategic planning something entirely unrelated?

It would be wise to start with incidences in literature attempting to integrate the organisation with the board/executive team in the strategy-making process, with the aim of improving firm performance. Minztberg (1978) has pointed out the possibilities of the strategy-making process with increasing involvement from members of the organisation, and only supported by the top management. Influenced by this work, (Hart, 1992) even advocated an integrative framework of five modes – combinations of which could be used by firms – ranging from being entirely top-management-driven to only being supported by the top management (as previously outlined by Mintzberg). Fama and Jensen's seminal work (1983) even bifurcated the decision management from decision control between the executive team and board, respectively. Despite such egalitarian and varied approaches, popular and practitioner outlook choose to rest the strategy-making hat on the responsible head of the board. It is this normative approach that has been the underlying assumption in this research.

Of those that admitted a board's role in strategy-making, many scholars traditionally associated governing boards with incidental strategic involvement, wherein strategy-planning and decision-making were not in their immediate purview. Theories like Managerial Hegemony (Mace, 1971) and Institutional theory (Selznick, 1957) viewed boards from perspectives which limited their role to support, or from the Agency theory (Jensen and Meckling, 1976) perspective, to control. It was only later, that the Stewardship theory (Donaldson, 1990) brought out the finer aspect of the board's strategic role. Ever since, studies have explored this aspect of the boards' role and contribution, and impact on the firm's present and future. While acceptance into their strategising role has been found, its detailed analysis and exploration could always benefit from further empirical investigation.

A study (Golden and Zajac, 2001) pointing to the evidence of boards' involvement in strategic change drew an insight of positive performance improvement of the firm, when the changes in strategy were brought forth with the consensus of the board. Further, McNulty and Pettigrew (1999) described three levels of involvement of boards clarifying that all boards may not be involved with the formulation of strategy; some may be involved in shaping it, while others may be involved in the entire process. These three levels are: (1) taking strategic decisions, (2) shaping strategic decisions, and (3) shaping the context, conduct, and content of strategy. All of these were influenced by the Agency theory's (Jensen and Meckling, 1976) control function, while the second and third were influenced more by the Resource Dependence perspective (Hendry and Kiel, 2004). Thus, we can see that integrated theories presented far better ways of addressing the board's role in strategy-making. Comparable results were confirmed by Stiles and Taylor's 2001 study of UK firms, which confirmed that board's role was to set strategic context and to maintain strategic framework.

Interestingly, the event of CEO succession proves especially useful for a board trying to influence strategic change, as inside successors are more likely than outside ones to maintain existing strategy (Tushman et al., 1985). It has been found that an individual director's home-firm strategy and diversification is likely to have an influence on their strategic preferences overall. Therefore, over time, as the tenure increases, CEOs may exert even more influence over strategy formulation (Westphal and Fredrickson, 2001). We can thus surmise that the director's respective past experiences frame their strategic preferences, which they implement at the new firm not only during strategy-making but also when it comes to director succession, in order to expand the sphere of influence and to choose directors whose preferences, they believe, would be aligned with theirs.

There are certain factors which provide rich insight into what would facilitate the board's active role in strategy-making, including reforming the board and its processes. One of these is the information flow between directors and managers whether through structures in place that enhance the communication or at the behest of directors proactively seeking such information. Another is choosing directors with optimal past experience of having served at other boards, and thus equipped with strategic problem-solving expertise (Rindova, 1999). Yet another could be to increase the frequency of meetings to enable more active participation (Rechner, 1989), and establishing specialised committees to look after specific interest areas. Finally, adequate decision-making processes, in place to facilitate strategy formulation, and a supportive CEO who encourages input from individual directors (Zahra and Pearce, 1990) would be other factors impacting their strategy-making role.

While crafting the actual strategy itself, the familiar and traditional process typically follows - setting the objectives that the firm wishes to achieve, then crafting the requisite strategy, and finally managing the required resources for the said objectives. This process inherently assumes a stable market environment, as well as no contingency factors affecting the firm itself. Perhaps this may be the reason many firms fail to adhere to the resources at hand or fulfil the objectives they set out to achieve. There is also a suggestion to reverse the planning process to start with available resources, which are then used to strategise and further establish objectives (Hayes, 1985). This potentially confirms that most firms choose their strategy based on three elementary components: ends, means, and ways (Hayes, 1985). The order and priority of these may differ for firms, but in essence the elements, more or less, stay the same. These are discussed in 2.3.3.

In real world circumstances, uncertainties and risks constantly go hand in hand. If potential uncertainties are unheeded, they may adversely impact a firm's competitive position (Elahi, 2013). Therefore, it is vital to consider the possibilities of uncertainty and take guarded risks, which are expected to reward in the future, and embed this rationale within the strategic planning phase. While boards have long been needed to be independent, today there is a growing cognizance for the need of them being both independent as well as intimate actors of corporate strategy (Oliver, 2000). How much or how little boards affect strategic change may eventually, ironically, be a board decision to hone over time. What stay undisputed, however, are the elements of such crafted strategy for the future.

2.3.3 Critical Elements of Strategy

Which elements constitute strategy for most organisations, could be guided by the definitions of corporate or competitive strategy that have been accepted by academics and practitioners over the course of time. Since the middle of the 20th century, the definition of strategy has entertained several and often varying perspectives. While Chandler's (1962) view of strategy was drawn from historical viewpoint in the military, which stated, "*the determination of basic long-term goals and objectives of an enterprise, and the adoption of courses of action, and the allocation of resources for carrying out these goals*.", Michael Porter in his book Competitive Strategy (1980), more than three decades later, defined competitive strategy as, "*a broad formula for a how a business is going to compete, what its goals should be, and what policies would be needed to carry out these goals*" (pp. 22). Knights and Morgan (1991) concluded that strategy is involved in the constitution (or redefinition) of problems in advance to offering itself as a solution to them.

The above definitions provide a peek into a wider spectrum of perspectives on the notion of strategy and what it encompasses. In the years that followed, several other approaches have been explored by scholars and practitioners alike. Minztberg et al. (1998) highlighted ten varied schools of thought on the topic, while Whittington (1993) outlined four conceptions of strategy which had varied implications on carrying it out. Kiel and Kawamoto (1997) demonstrated 32 different definitions of strategy, and the list would be even more populated today. Inherently, strategy is a shared perspective of the iterative process of objective-setting and resource-allocation (Burgleman, 1983; Noda and Bower, 1996). The object of enumerating the various names in the field of strategy and its genealogy is to point out the changing voice and view of the times.

Over time, therefore, while definitions have reflected the popular perspectives of the time, they have more or less done so in the familiar scope of 'ends-means-ways' elements as pointed out earlier (Hayes, 1985). Here, the ends referred to the established objectives, the means pointed to the resources available, and the ways meant the strategic process. Thus, any strategy-making process would inherently involve the three constituents of setting objectives, allocating resources, and developing the strategic route to achieving the same, the order of which would be contingent on contextual factors for any firm. A list emerges of the following elements which are critical to the nature of strategy-making at the corporate level:

2.3.3.1 Mission Development or 'ends'

Establishing the unique position of the organisation with respect to its mission, vision and direction are elementary steps for its foundation. While it may essentially be episodic in that it needs to be conducted at the commencement of the company, it will also need to be iterative to keep itself updated as and when changes are made to its distinctive elements. While other roles or degree of involvement may have found disparate opinions in literature, this particular step in strategy-making is distinctly within the purview of the board. (Zahra and Pearce, 1990) study also helped outline how the board participates in the crucial task of developing the business concept, identifying new business opportunities, and setting long-term objectives.

These would include financial objectives amongst other overall objectives the firm wishes to achieve (Roundtable, 1990). It would also set in place the company's aspiration with respect to all its stakeholders - including investors, customers, suppliers, vendors, employees, and communities (Nadler, 2004). Company mission (Lauenstein, 1982) thus forms the first and least debated of the process of strategy-making. Identifying the characteristics unique to the company, framing the mission and vision statements of the company, accordingly, classifying the business position, and articulating the objectives which the company wishes to fulfil, thus, together, form the most elementary first step of a board's role in crafting their corporate strategy.

2.3.3.2 Resource allocation or 'means'

Another critical element in strategic planning is deciding the allocation of resources available as well as those that are emerging over the course of business. Resources under consideration here would have a wide range in the entire spectrum of capital – social and human capital, financial capital (Clarysse, Knockaert and Lockett, 2007), technical capital, intellectual capital, and institutional capital. Depending on the strategies the organisation wishes to craft, it has to decide on a combination of resources or characteristics which are of great significance and when (Hofer, 1975), and then marshal those. Important here would be to note that having access to the requisite resources and being able to use them in the way intended are both equally important in being able to strategise which resources are needed. Using an opportunity to control the firm through manipulating the above two were pointed out by (Frooman, 1999) as withholding and usage strategies, in the context of resource control.

Outside non-executive directors, especially, have been relied on for the access to resources (Daily, Dalton and Jr., 2003) that they allow. Having existing networks external to the organisation - in terms of raw material, talent pool and associations – and also through their past and other current associations, are valued sources of resources which board directors enable for the organisation. However, this is not to undermine the resource-linking capabilities of inside directors, which are known to be an important determinant of a company's future survival and growth (Clarysse, Knockaert and Lockett, 2007). In case of certain sectors of industries like technology firms, which are often especially resource-poor (Clarysse, Knockaert and Lockett, 2007), as the technologies evolve sooner than firms could financially keep up, such access to resources is crucial. Thus, a firm's resources rightly incorporate a critical element in its strategic process.

2.3.3.3 Strategy formulation or 'ways'

This critical element lies at the foundation of the entire strategy-making process. Referred to as the traditional planning activity (Lorange, 1980), it is the means of achieving the set objectives of the organisation and may even be considered as the positioning through strategy that organisations attempt to use to sustain performance into the unforeseeable future, with (Bowman and Hurry, 1993). With a futuristic view, it considers the idea of investment pre-commitment (Ghemawat, 1991) as vital to deciding the strategic stance of investment planning. At the confluence of external and internal environments orientation, strategic planning pitches the use of competitive strategy for optimum use of resources. Developing core competencies – portfolios of skills and capabilities (Prahalad and Hamel, 1990) - thus would be an effective way to address external environment issues of the future. In essence, it is the ultimate step where the objectives set in step one and the resources accessed in step two, are strategically put to use.

Further, gaining competitive advantage that is sustainable through developing relatively inimitable resources (Bowman and Hurry, 1993) which may be non-substitutable, lies at the heart of the strategic planning. Adopting the Resource-Based View of the firm, the strategy development process allows the organisation to identify the conditions where it can even pitch its corporate governance as a source of its competitive advantage (Barney, Wright and Ketchen, 2001). While it is important to clarify that corporate governance on its own may not be an advantage over the firm’s rivals, the way it is implemented and practised, however, may set it apart from its competitors and thus be a competitive advantage. Thus, this element of strategy allows the firm to differentiate itself from its competitors and also impacts its survivability. Hence, outlining its competitive advantage through its strategic positioning is a key component of strategy development/formulation.

2.3.4 Strategy Execution

Stiles and Taylor (2001) argue in favour of the boards’ strategic tasks, including execution of strategy; hence board dynamics have considerable influence. Board dynamics (like demography, job-related diversity, proportion of outsiders, board size and board tenure (Forbes and Milliken, 1999) have a vital role to play in board processes. While (Mcnulty, Zattoni and Douglas, 2013) support the view of control and collaboration aiding effectiveness, others like (Heemskerk, Heemskerk, and Wats, 2017) have vouched for a positive relationship between task conflict and cohesion. However, before execution it is imperative that boards are competent to craft the appropriate strategy best suited for their organisation.

Practitioner reports have highlighted the importance of governing boards to focus on strategy, if they wish to move towards growth and innovation. For this, including a strategic mindset of the board is key, which would involve hiring experts with rich industry experience and experience of market and industry knowledge (Carey and Patsalos-fox, 2006). This importance for board dynamics and decision-making has been supported by (Useem, 2003) with the view that to optimise shareholder benefits, it is of significance that companies pay attention to their board composition and policies.

It is increasingly evident that cybersecurity campaigns, while maybe intended for an organisation, sometimes have the potential to impact not just the intended victim but the society/state at large. Besides the reputational (De Minville, 2020; Gale, Bongiovanni and Slapnicar, 2022), legal and financial losses (Nolan, Lawyer, and Dodd, 2019), it also exposes the vulnerability of those overwhelmed by the attack. Thus, the directors involved in strategising for cybersecurity often depend on metrics and frameworks (existing or customised ones) to define their firm’s cybersecurity status and to prioritise investment (Moore, Dynes, and Chang, 2015). Extending the stewardship role of directors, as (Forbes and Milliken, 1999) point out, when directors are seen as stewards of organisational resources which may have a larger impact, the significance of their responsibilities becomes apparent.

2.3.5 Competitive Advantage Unpacked

In literature, Resource-Based View (Wernerfelt, 1984) has been credited with accounting for competitive advantage as a critical element of corporate strategy. It advocated gaining competitive advantage through the firm's internal core resources and competencies (Ghezzi, 2013). Later, the Stakeholder theory (Freeman, 1984) improved upon a missing feature of the Resource-Based View (Wernerfelt, 1984) by guiding *how* firms should manage resources in order to achieve competitive advantage (Priem and Butler, 2001). Some studies also integrated Resource-Based View (Wernerfelt, 1984) with the Resource Dependence Theory (Pfeffer and Salancik, 1978) on account of their common foundation in organisational resource endowments to explore how creating resource interdependencies around critical resources could affect the advantage derived from them (Hillman, Withers and Collins, 2009). These theories could be considered the foundational influence for this vital element of corporate strategy.

While we discuss the construct of competitive advantage, it is vital to highlight the important terms of the field which are popular within the realm. To begin with, *sustainable* competitive advantage (Oliver, 1997; Huang *et al.*, 2015) has been desired by strategists, as labouring to secure resources for competitive advantage alone is not sufficient. It is key that the organisation is able to appreciate sustainability of such benefits. From this perspective, sustainability would seem like an advantage that would continue for a long time (Porter, 1985; Jacobsen, 1988), as the term *sustained* entails multiple time periods (Arend and Lévesque, 2010). However, a sustained competitive advantage is not so simplistic in nature. According to the Resource-Based View (Wernerfelt, 1984), a resource could potentially be a competitive advantage which will be considered *sustained*, only when it meets all of the following four conditions (Barney, 1991):

- *valuable* – it exploits opportunities and/or neutralised threats in the firm's environment.
- *rare* – rare among a firm's current and potential competition
- *inimitable* – imperfectly imitable (highlighted by one or all of three factors – it is dependent on unique historical conditions, the link between resource and competitive advantage is causally ambiguous, and it is socially complex)
- *non-substitutable* – there cannot be strategically equivalent substitutes

The above yardstick has been the industry norm for identifying potential sources which have the capability of being sustainable competitive advantages. Another important term was *core* competitive advantage. This essentially functioned as a yardstick for a resource or competence to be considered a potential source of competitive advantage. Similar to what enabled a potential source the possibility of being sustainable, a study (Collis and Montgomery, 1995) proposed the idea of five tests for a resource to be considered core; these were – inimitability (hard to copy), durability (how quickly does it depreciate?), appropriability (who captures the value that the resource creates?), non-substitutability (can a unique resource be trumped by a different resource?), and competitive superiority (whose resource is really better?). Thus, definitions and terms have evolved in the genre, while they have been similar in checking a resource's ability to be genuine sources of a firm's competitive benefit.

The idea of a competitive advantage arises from the potential heterogeneity of resources, which create distinct strategic options for a firm that, over time, enables its managers to exploit distinct levels of economic rents from (Peteraf, 1993). She further highlights four cornerstones which are essential conditions to be met for a firm to be able to enjoy competitive returns. According to her, these are: (1) heterogeneity (firms with varying capabilities with respect to resources – some have some superior resources; others do not); (2) ex-post limits to competition (condition of heterogeneity must be relatively durable to add value); (3) imperfect mobility (resources which cannot be traded); and (4) ex-ante limits to competition (limited competition to the position of superiority in the first place). Thus, we see that despite the same foundation (resource view), scholars have found different yet some similar features, which differentiate a resource as one providing competitive returns.

Other scholars since have revised their versions of these conditions, and their requirements have evolved over the last few decades. For instance, these resources, further, are mostly expected to be knowledge-based resources in the form of information inputs, know-how and capabilities that organisational members draw on when searching for innovative solutions (Dosi, 1988). Over the course of time, such resources have the greatest potential to serve as sources of sustainable competitive advantage (Coff, 1997; Grant, 1996; Kogut and Zander, 1992). This is because they are the unique firm-specific features, which would fulfil the earlier stated four requirements (Barney, 1991) – valuable, rare, inimitable, and non-substitutable – enabling its sustainability as a potential source of competitive advantage.

Meanwhile, certain scholars have argued that without the existence of proper governance mechanisms and trust between a firm and its employees, a firm may not be able to exploit the economic rents arising out of its heterogeneous resources; this potential may not be realised. Makadok (2003) explains that to better appreciate how firm-specific resources have the potential to function as competitive advantages, both the firm's resource base as well as its governance mechanism need to be working effectively in tandem. Thus, firms need to be able to bridge the gap between potential and realised economic rents by achieving economic performance through the adoption of governance mechanisms which mitigate employee underinvestment in firm-specific knowledge-based resources (Carnahan, Agarwal, and Campbell, 2010). Another factor for realising such economic rents is pointed out by (Barney, 2001) while citing the need for imperfectly competitive strategic factor markets vis-à-vis neo-classical microeconomics studied by Ricardo (1817) over two hundred years ago.

Thus, though theoretical origins may be varied, they help understand and address the question of creating an advantage unique to the company, which would allow success over its competitors. While it could be achieved through various means for the purpose of creating economic rents (Barney, 1991), it lies in the notion of capturing value by excluding rivals from opportunities (Adner and Zemsky, 2006). As such, it could be of two types – temporary and sustainable - while, understandably, the objective is to attain sustainable advantage so as to reap the benefits of crafting strategy around core competencies. Traditional view revolved around resources and value creation, which are demand-side components; sustainable competitive advantage could be created out of supply-side elements, like marginal utility and consumer heterogeneity across market segments (Adner and Zemsky, 2006).

This notion adds another layer of complexity to this field, as well as augments the perspective of the field of competitive advantage. Thus, different views and perspectives have dominated the domain of competitive advantage since they were brought to focus a few decades ago. The construct of competitive advantage is further explored through the several ways in which firms in the market have differentiated themselves from their competitors. Based on popularly chosen tools, certain definitions have come to be accepted as the norm and they have the potential for businesses to not only distinguish themselves from their rivals, but also differentiate their success stories from those which struggle to survive the test of time. Through scholars' exploration and practitioners' trial and elimination, in contemporary times, there are a few popular tools of competitive advantage which have been outlined in the next section.

2.3.6 Sources of Competitive Advantage

Competitive advantage studies abound in strategic literature. Advocating differing elements and routes to achieving and maintaining it, scholars have discussed this fascinating topic that would bring organisations one step closer to long-term success. Two interesting approaches are suggested by proponents of the Industrial Organisation theory (Bain, 1959) and Resource-Based View (Wernerfelt, 1984) which, at their core, are concerned with competitive success (Huang *et al.*, 2015). The contrasting element of these two approaches is their orientation - IO (International Organisation theory) economists propose looking inward (within the firm) to achieve such an advantage while RBV (Resource-Based View) supporters have a more outward focus (market orientation) as an answer. There would be other perspectives, too, for analysing competitive advantage but they have not been able to find adequate success in being recognised as other possible approaches to this subject area.

There are those who argue that a firm's stakeholder network can be a source of sustainable competitive advantage (Harrison et al., 2010). By potentially drawing on the network of their stakeholder relationship to widen and strengthen access to resources, a firm may be able to form a basis for competitive benefits. This would be one of the two essential components of a firm's competitive advantage, as pointed out by other scholars – market position (or resources) and performance (or profitability) (Huang *et al.*, 2015). In the 4.0 economy, however, the perspective of competitive advantage has also widened. Views of this evolved digital landscape call for finding competitive benefits from data as a strategic asset (considering it is the new oil for the information economy (McAfee and Brynjolfsson, 2012; Perrons and Jensen, 2015; Varian, 2014)). Therefore, the way it is gathered, analysed, used to make decisions, and develop (Nagy *et al.*, 2018) and perhaps secured (Kosutic and Pigni, 2020b) are going to be instrumental in deciding the potential competitive advantage one firm has over the others in the coming future.

However, to consolidate the comprehensive list of possible sources of a firm's competitive advantage may not even be a feasible option, as the source of potential competitive advantage is a subjective choice for each firm. Firms will need to strategically choose their competitive advantage depending on multiple factors which could be industry sector of operation, stage in life cycle, public vis-à-vis ownership, geographical base of operations, influences of demographics of board members, and access to resources. Meanwhile, significant, and popular instances from the growing literature of this subject have been compiled to identify how firms decide the source of their benefits over their rivals. The following are the most popularly vouched-for potential sources of achieving competitive advantage:

2.3.6.1 Intellectual Capital

Intellectual capital is a constantly evolving topic despite its popular base in research (Guthrie et al., 2012). Defined as the "*the sum of everything everybody knows that gives it a competitive edge. Intellectual capital is intellectual material, knowledge, experience, intellectual property, information that can be put to use to create value"* (Dumay, 2016, pp.169). Klein, Crawford, and Alchian (1978) regarded intellectual capital as knowledge, expertise and associated soft assets of a company. Resource-Based View has recognised three diverse kinds of firm resources – physical, human, and organisational capital resources (Barney, 1991). Intellectual capital would inherently be placed in the middle of two of those resources – human and organisational.

Human capital has been understood to consist of a combined stock of knowledge and skills which individuals develop through education, training, experience, and interactions among their peers (Becker, 1964; Coff and Kryscynsky, 2011; Mahoney and Kor, 2015; Nelson and Winter, 1982). Some scholars, from the Resource-Based View perspective, have argued that sustained competitive advantage can accrue from cumulative human capital. One aspect of intellectual capital is captured in the collective knowledge of this human capital source (Hsu and Wang, 2012; Bana *et al.*, 2022). The other is part of the organisation's structural resource, including its IT assets like systems and processes (Barney and Clark, 2007a), which enable the flow of knowledge through the organisation.

Organisations are increasingly relying on intellectual capital over mere tangible assets. Information and communication technology is a stream which has helped redefine economic value creation through intellectual capital (Sallos *et al.*, 2019). Thus, in the technologically advanced times of today, many firms rely on their smart, cutting-edge, intellectual capital which helps distinguish them from their competitors in the eyes of their customers. However, the inability of a measurement system to cope with the intangible nature of intellectual capital (Hsu and Wang, 2012) may be a glaring limitation of it. While investing in it is not a matter of choice in the 4.0 economy, strategic managers would need to be especially careful while attempting to associate firm performance with an intangible construct like intellectual capital.

The lack of an appropriate measurement system is indeed a drawback for an otherwise rich source of competitive advantage. Additionally, on its own, it is also limited in allowing a firm the possibility of drawing economic rents from it over their competitors over extended periods of time. Especially, with respect to the issue of cybersecurity and the way boards could strategise for safeguarding the organisation against future cyber vulnerabilities, intellectual capital falls short of a holistic advantage that addresses the entire challenge. Without complementary IT-based assets, intellectual capital (Sallos *et al.*, 2019) could very well be considered inadequate.

2.3.6.2 Dynamic Capabilities

The primary strategic management challenge in the knowledge economy has been identified as being both a competitor and an evolver (Leibold et al., 2002). Such a perspective of strategy requires a firm's sustainable advantage that can exist even in swiftly changing external environments. The Resource-Based View of the firm was able to bring forth a potential solution. It encouraged the idea of viewing firms in terms of resources rather than their products. It suggested two possibilities of attaining competitive advantage – either delivering product benefits perceived by customers or process benefits which allow lower unit costs (Bowman and Ambrosini, 2003). An extension of that view was introduced through the Dynamic Capability view (Teece, Pisano and Shuen, 1997; Eisenhardt and Martin, 2000), which facilitated the notion of resource creation in the future. It viewed capabilities as resources which were cultivated over time (rather than being bought) (Teece, Pisano and Shuen, 1997), thus making strategic choices of resources and long-term commitments of competence development.

Previous perspectives of strategy-making viewed through a limited lens of either competitive forces (finding a position in the industry from which to best defend itself against the market forces) or strategic conflict (choosing strategic direction so as to influence behaviour or actions of rival firms) (Teece, Pisano and Shuen, 1997). Using timely responsiveness, product development and managerial agility to reinvest internal and external resources, a firm could use its dynamic capabilities to achieve competitive advantage. This view considered redeploying existing resources as per the changing requirements created by the market/circumstances, and hence is largely environment-driven rather than through a firm's inherent resource-led choices. This perspective of drawing a competitive advantage from an external source could enable a firm considerable success, as it strategically chooses to differentiate itself from its competitors.

Turbulent external conditions make a firm's advantage unsustainable and unpredictable (Izadi, Hossein, 2017). In such a scenario, since dynamic capabilities allow a firm to develop its advantage over a period of time, it essentially has an edge over its competitors in such unsavoury market conditions. Thus, it may be viewed that the advantage of dynamic capabilities is that of enabling a firm to extend, modify or create abilities which support its 'earning a living' capacity (Winter, 2003), even during tough external circumstances. There could be several ways in which a firm could develop its dynamic capabilities, some of which could be surmised in the following six ways (Bowman and Ambrosini, 2003): (1) reconfiguration of support activities; (2) reconfiguration of core processes; (3) leverage of existing resources; (4) encouraged learning; (5) provoked learning; and (6) creative integration.

However, even developing such evolved resources, which are sustainable despite unfavourable external conditions, cannot be continuous in nature. (Barney and Clark, 2007c) point out that the ability of a firm to create new capabilities is assumed to remain constant and, therefore, question the 'dynamic' nature of these resource-based capabilities. Furthermore, in cases where dynamic capabilities require an expensive change, the benefit derived may not be justified by the cost incurred in certain cases; hence it may not always be necessarily advantageous (Winter, 2003) to adopt this route. While it proposes novel ideas and helpful suggestions of dealing with competition, it also led to certain scepticism regarding its value offering.

This research is attempting to develop a framework of identifying how firms strategically decide to address cybersecurity challenges, while exploring if they could derive a competitive advantage from it. The cost of having to change the capabilities in the future invites doubt as to its applicability as a reliable source of gaining significant competitive advantages from it, in the long-term. In the absence of much-needed reliability and sustainability as its strengths, dynamic capabilities do not offer the benefits this research wishes to investigate further. Hence, a more appropriate potential source is searched for.

2.3.6.3 Risk Management

The 4.0 economy is not only dynamic, but it could also even be considered volatile as far as markets and the business world are concerned. Owing to such volatile nature of business, there is an argument advocating investing in risk management as a strategic choice, hoping to attain competitive advantage from it. (Elahi, 2013) recommends doing it in one of four ways: choosing to be stronger in dealing with a disruption, seeking riskier business choices with higher potential benefits, effectively managing day-to-day fluctuations in a stable environment, or creating a resilient image. Michael Porter (1985) in his book highlighted two ways of effectively managing competition to gain competitive advantage – cost advantage and differentiation (creating value). Risk management, it could be argued, fortifies the business by reducing costs and thus creating value for the customers, thereby allowing it to gain a competitive edge over its rivals.

Uncertainty is usually associated with risks and costs, and while that may be its normative nature, addressing higher levels of uncertainty also provide opportunities (Courtney et al., 1997) which, adequately managed, could lead to potential competitive advantages. Especially, the contemporary world of 4.0 economy is characterised by complexity and uncertainty, which could be better managed by holistic risk governance (Leonhardt and Wiedemann, 2015). Enterprise risk management, as a concept, found much popularity in the 1990s, but it took time finding practical adoption. Slywotzky and Drzik (2005) witnessed many organisations incorporating enterprise risk-management as part of compliance procedures; however, compliance-led strategic choices may not be the most conducive to competitive advantage, as discussed previously.

In his theory of ‘risk society,’ German sociologist Ulrich Beck (1992), while not discussing cyber-threats, elaborated on liberal modern societies which increasingly relied on technologies. This, according to him, has the potential of constantly producing new risks. Thus, not only organisations, but even governments in North America, Europe, Russia, China, and other parts of the world (Eriksson and Giacomello, 2006) are investing in the management of risk. However, for a firm it is crucial to decide whether the origins of its inclination to manage risk are a response to the external stimuli of potential threats or a preventive measure to safeguard itself against them. As a preventive measure, it has the potential to create a competitive advantage. However, in the contemporary scenario, a firm would have to envision risk, which is potentially several generations ahead of its time, to enable secure risk-management solutions. Otherwise, it is only ensuring as much protection against business risk (Bickley, 1959) as its competitors, and not gaining any advantage over them.

Risk-management as a construct is certainly a positive sign, with the firm choosing an assertive stance to potentially secure against that weakness, as well as gain advantages in the market. However, as pointed out earlier, risk-management in this way, while being an effective way of elongating the firm’s life and chances of survival, may yet fail to potentially work as a source of sustainable competitive advantage. For an organisation to succeed over time and maintain its dominance in the market, it needs more than risk compliance from which to derive the competitive edge. It needs to strategically choose an asset it can utilise over extended time periods, among other qualities, to draw that benefit. For this research into cybersecurity especially, merely attempting to guard against potential vulnerabilities is inadequate in the long-term. It has to be able to develop competencies and capabilities to reliably ward off the danger of cyber-attack and all the collateral damage it brings with it.

2.3.6.4 Combination of IT and ICT/Cybersecurity

The focus on technology in strategy and the growing tendency of firms to define themselves in terms of technologies (Wernerfelt, 1984) demonstrates that even far back in 1980s, when the Resource-Based View (Wernerfelt, 1984) first came into prominence, Information Technology (IT) had gained significance as a reliable and vital firm resource. While the advancements in the field of IT and Information and Communication Technologies (ICT) have been considerable in the past forty years, the reliability factor has survived. Furthermore, IT and its several aspects offer opportunities to provide temporary as well as sustainable competitive advantages. In the technology advanced era of the 4.0 economy, having a strong internet economy has contributed to a higher proportion of the UK's GDP than any other country in the G20 (Cordes and Stacey, 2017); hence, offering it and firms within the UK a fortuitous infrastructural competitive advantage. Further, sound technological firm resources have been found to trump over strong market conditions to provide sustainable competitive advantage to firms (Huang *et al.*, 2015), thus lending support to the idea of developing strong internal IT resources (Barney and Clark, 2007a; Pavlou and Sawy, 2010).

Barney and Clark (2007a), in their illuminating paper, discussed five attributes of IT as resources with potential competitive advantages. These were customer-switching costs (related to IT supplier specific investments), access to capital (financial resources required to develop IT), proprietary technology (needed to be kept secret), technical IT skills (related to programming languages or software), and managerial IT skills (both skills of IT managers to understand their stakeholders, and their ability to work with them). Of these five, they believed only the last was capable of being a sustainable competitive advantage – managerial IT skills. In the decade since, interestingly, the ways of exploiting the firm's IT-based competitive resources have evolved to using socially complex resources. The world of interconnected networks today has created more complexities which perhaps require organisations to re-evaluate their investment in, and strategies of utilising their IT resources.

While many firms may have access to the same physical technology, only a handful of them may possess a judicious mix of social relations, cultures, traditions, etc. (Wilkins, 1989) which sets them apart in utilising the said technology as a source of competitive advantage. The unique aspect of selective hiring, training, socialising, and supporting within a firm (Banalieva and Dhanaraj, 2019; Bana *et al.*, 2022) supports its human capital in developing firm-specific advantages. Further, in the digitalised world of today, the firm's managerial IT resource possess the know-how to operate with, maintain, and extract the most value from modern technologies (Banalieva and Dhanaraj, 2019), which aids its potential as a source of sustained competitive advantage. This further exemplifies the managerial skills insight of (Barney and Clark, 2007a) made above.

Mata, Fuerst and Barney (1995) further lend support to the above idea of the most sustainable aspect of IT as a competitive advantage being the management skills. They argue that these skills are heterogeneously distributed, besides being influenced by a firm's particular history, and the intricate relationship between the IT function and other firm functions, and that of the IT function with the firm's suppliers. Potentially taking it a step further to imagine a firm that would hire an outside board director with strong expertise in IT (Landefeld *et al.*, 2017), as opposed to one which only hires IT experts at lower levels of operation, offers a keen insight. The first case would enable the director to influence not only the firm's access to the latest technologies and other high calibre technical talent (Bana *et al.*, 2022), but also the customised and relevant strategic stance needed by the firm, to stay atop its competition. While the second one will be limited to managing IT related incidents and choices at an operational level. Between the two, it is simple to imagine which would be a potential source of competitive advantage.

Over time, the scenario may have evolved quickly to keep pace with the rate of change as technologies constantly evolve and even change. However, the advantage offered by an IT foundation is that the firm is able to not only defend itself against cyber-threats, but also proactively manages it (Hubbard *et al.*, 2021), thus allowing a sustainable competitive advantage. This is a fitting example of implementing a strategy that exploits internal strengths by responding to external opportunities - while neutralising external threats - and avoiding internal weaknesses (Barney, 1991). This implementation of the SWOT (strength, weaknesses, opportunities, threats) model in the context of sustainable competitive advantage certainly adds another perspective to viewing the strategic management of a firm's IT resources.

The discussion above aids the understanding and appreciation of exploiting a firm's collective IT resources as a source of sustained competitive advantage. This perspective is particularly useful for the purpose of this research as it draws on a strong insight relating the firm's IT with its human capital (Wright, 2021). IT systems and processes, novel, state-of-the-art and innovative as they may be, may be imitated and/or run the risk of being out-dated over the course of time. Similarly, human capital alone would not have fulfilled the requirement to be able to be strategised adequately for cybersecurity. It is only when these IT systems and processes, and the human resources who effectively utilise such hardware and software, are combined (Barnes, 2019; Wright, 2021) that the category of a strong IT foundation becomes the most reliable source of sustained competitive advantage, in the knowledge era of today.

2.3.7 Summary of Strategising for Competitive Advantage

The definition of strategy itself has evolved with the changing times, which means the way firms have chosen their long-term strategic plans, has also been affected. Right from deciding who crafts strategy – the executive committee or the board – to how involved boards are in strategy-making, the matter has often invited much intellectual debate. Thus, strategy has been a popular area of research for scholars and investigation for practitioners. Boards, through corporate strategy, need to constantly identify and update the ways in which they wish to achieve success over the firm's market rivals. Within this realm, competitive advantage may be considered the most significant of its components, as it allows academics to propose what would lead firms to achieve competitive success and for industry experts to verify whether or not the above was proven true. Over time, for competitive advantage, several potential sources have gained popularity and significance.

However, in the increasingly technology-driven climate of today, firms across the industry sectors may do well to equip themselves with tools of an IT-enabled advantage so as to allow them chances of long-term survival, and even success. With ample evidence around today, there are commonplace short-term success stories of companies achieving quick success, and in quick succession, but also succumbing to any number of internal or external events. In such a scenario, sustainable competitive advantage, which truly affords a firm significant benefits over its rivals - which carries all characteristic traits of being sustainable as highlighted by (Barney and Clark, 2007b) - may very well arise out of a firm's ability to safeguard itself against potential cyber-threats (Shong, 2019; Kosutic and Pigni, 2020b). For a firm, while it may be impossible to eliminate all threats (Peng, 2018), the endeavour has to be to find ways of effectively and efficiently reducing its vulnerabilities and developing strengths which secure its cyber realm.

2.4 Cybersecurity

The third significant pillar for this research is cybersecurity, in the broadest sense. With a general lack of a commonly accepted and concise definition in literature (Craigen, Diakun-Thibault and Purse, 2014), the usual connotation for cybersecurity ordinarily tends to be associated with and often limited to technology. The attempt to protect and safeguard an organisation's cyber assets or infrastructure may be interpreted as cybersecurity for the purposes of this study. This often does involve an integration of the physical and cyber securities of the assets (Barnes, 2019), in the course of securing the organisation. This section explores cybersecurity through a temporal comparison, with respect to the evolving perspectives of cybersecurity with the passage of time. Understanding cybersecurity and its significance through various time periods, enables appreciating its value in the future. This would help explore apt resolutions for the growing concerns of the field. Moreover, appreciating the way it is managed and/ or governed in organisations supports the third important pillar of this study.

2.4.1 Overview

The world of today is increasingly dependent on technology. Understandably, interconnectedness is one of the essential underlying assumptions of modern society. The internet, being the most popular infrastructure as well as a communication medium (Eriksson and Giacomello, 2006), has enabled us all to overcome physical boundaries. Since its inception in the 1960s, it has proved itself to be a remarkable and ubiquitous technology, which regrettably remains insecure and prone to exploitation and subversion (Barnard-Wills and Ashenden, 2012). Geography, sponsor, age, and objective – all of these are rendered insignificant if the actors are adequately motivated to connect using the information technologies of contemporary times. As such, this makes for a sinister medley of potential threats, which are now well-known as cybersecurity concerns.

While the definitions of the term may be varied (Craigen, Diakun-Thibault and Purse, 2014), what is undisputed is that cyber-*insecurity* begins from a vulnerability, flaw, or weakness that an adversary learns about (Finnemore and Hollis, 2016)**.** Individuals, corporates and even states are putting their best minds to develop ways to pre-empt concerns of this nature and address them. Especially, organisations the world over are finding novel means of addressing this momentous topic. How they manage cybersecurity, and what it augurs for the future, is discussed in this section.

2.4.2 Is Cybersecurity an Element of Compliance or Stewardship?

The board's function of oversight (Lunn, 2014) can be covered through two sub-functions – compliance and stewardship. Corporate governance reforms are forcing boards to focus increased attention on compliance, even at the expense of strategy (Hendry, Kiel, and Nicholson, 2010). While the compliance element ensures that basic best practices are carried out, which essentially answers the question - 'if the boards are even involved in cybersecurity management', on the other hand, stewardship warrants that the boards go a step beyond the immediate monitoring measures and ensure that cybersecurity is pre-emptively prepared for, and not only managed. This debate is central to understanding how firms today view cybersecurity. When accounted for by size, stage in lifecycle, geography, or industry sector, do different enterprises approach this topic differently? Or in the 4.0 economy, is every firm brought to the same level-playing field of approaching it in a universal fashion?

In the lifecycle of how cybersecurity has evolved over the last few decades, the perspective to approaching it has evolved as well. Initially, the need to safeguard online or virtual assets was primarily faced by certain sectors like dotcom firms, internet companies or banking sector enterprises, which either had businesses in the internet space or stored confidential information of customers/stakeholders online. Investments in cybersecurity measures were perhaps approached with an 'if needed' basis or perhaps to ensure risk reduction. A study (Moore, Dynes, and Chang, 2015) conducted on several US and European firms, to better understand their respective cybersecurity perspectives - through investigation with their CIOs and managers - revealed interesting results. It brought to light two very insightful revelations – first, that the US firms were more updated as well as prepared than their counterparts in the UK and Europe. The second was that most firms viewed the need to invest in cybersecurity primarily as a response to either reducing risk or fulfilling compliance requirements. However, it must be noted that between the time of the study and now has already been more than five years which, within the perspective of the subject area, is a considerable time gap.

While it highlights how firms viewed cybersecurity as a compliance issue circa 2015, it also raises certain vital questions. What is the evolution of the board's role in cybersecurity planning today, as well as does the difference in industry, firm size or lifecycle stage influence its cyber strategies? And most importantly do they still view cybersecurity from the perspective of adhering to a role of conformance? Literature has evolved along with cybersecurity as a topic. The results seem to be maturing as well as the responses from practitioners, policymakers, and academics alike. Another investigative study (Schwab and Poujol, 2018) with over 300 international professionals revealed that over half of the respondents confirmed the prioritised view of cybersecurity, as well as the strong involvement of their board and top-management teams in strategising for cybersecurity.

Hence, we realise that the perspectives on cybersecurity are simultaneously evolving with the changing times, strengthened by the organisation's association and dependence on information and communication technology for the functioning of their business. As the threat of cyber breaches becomes potentially more probable for each firm (Ablon and Libicki, 2015) - while nothing could prepare wholly for the avoidance of novel attacks - organisations realise that a robust cyber-defence preparation could mitigate the impact on their financial and reputational exposure (Kewell, 2007). Cybersecurity today warrants more attention than merely ticking the box of risk compliance as a future response to incidental threats. It is, thus, increasingly a matter of priority owing to the interconnectedness (Haleem *et al.*, 2022) of devices, networks, and firms. Understandably, organisations do not want to wait to be breached to address the issue. Keeping a metaphoric fire extinguisher/fire blanket in place, securing a fire alarm, along with following fire safety protocols, are crucial for potentially approaching this metaphoric fire hazard.

2.4.3 Historical View of Cybersecurity

To address issues of cybersecurity, it would perhaps be helpful to better appreciate the term and its genesis. Viewing the past may even allow us some potential insight into unlocking the opportunities it possesses, which will help us manage the threats. Cybersecurity as a construct has already been there for a few decades. Perhaps it could be assumed that as soon as *cyber* was coined in popular usage, it was shortly followed by academics and their growing concerns about the potential of its security-related vulnerabilities.

There may be multiple perspectives on when and how the issue of cybersecurity first came to be recognised and by whom. However, it would perhaps not be incorrect to imagine that, as early as the 1970s, as the field of information technology was developing, certain foresighted academics and industry experts were able to identify and recognise the potential for it to cause vulnerabilities in the then-future. This was rightly so; as technologies led to the progression from an industrial society to an information society (Alberts and Papp, 1997; Henry and Peartree, 1998), the fear of defencelessness led to the early concerns for cyber-threats. The adjacent Figure 2.2 demonstrates this progression.

The United States of America has been highly active in this field both from an academic viewpoint as well as from that of the industry. However, in Europe, the Swedish government received a report from Tengelin (1981), which emphasised the main risks of a networked society, including those from the dependence on international vendors as well as threats from hackers' raids. Popular culture has had much to contribute to arousing interest from scholars as, a few short years later, with the blossoming of the genre of science fiction, a subgenre of 'cyberpunk' developed through popular novelists like William Gibson. He coined the term *cyberspace* in his novel, Neuromancer (1984), which found popularity in academic works soon after.

Before the end of the decade, the world of cyber had caught the interest of other pioneers in the field, like sociologist Manuel Castells, who foresaw the significance 'information' was going to enjoy as the primary resource in the newly emerging *knowledge economy* (Castells, 1989). Crucial services like banking, air travel, water or electricity distribution began to rely increasingly on the foundation of functioning information technology. Early in the next decade, work by the RAND organisation was making progress in the USA, which was aimed at research and analysis for supporting the American armed forces. RAND analysts, John Arquilla and David Ronfeldt established *cyberwar* as a key concept of information technology in military activities in their paper in 1993 (Arquilla and Ronfeldt, 1997). Being discussed in national security mandates, cybersecurity was next brought to focus by the White House, under the Bill Clinton administration, which was key in popularising *information highway*.

As the world was growing increasingly accustomed to information technology and an age of faster and smoother communication, the reliance on computers had also increased. Volti (1995) talked about how this had led to optimistic visions of potential technical solutions to societal problems, or *technological fixes*. Accompanied by feelings of fear, popular culture through movies of the time depicted evil technologies taking over the world, symbolic of the fear of technology and all that it would bring (Eriksson and Giacomello, 2006). Simultaneously, progress in sociology studies was increasingly finding itself mentioning information as a cornerstone of modern societies, coupled with associated fears. Castells (1996, 1997, 1998, 2000) even dedicated a trilogy to the dawn of a globally networked society, where transnational organised crime would be a momentous potential threat to global security, expressing concerns linked to interconnected technologies.

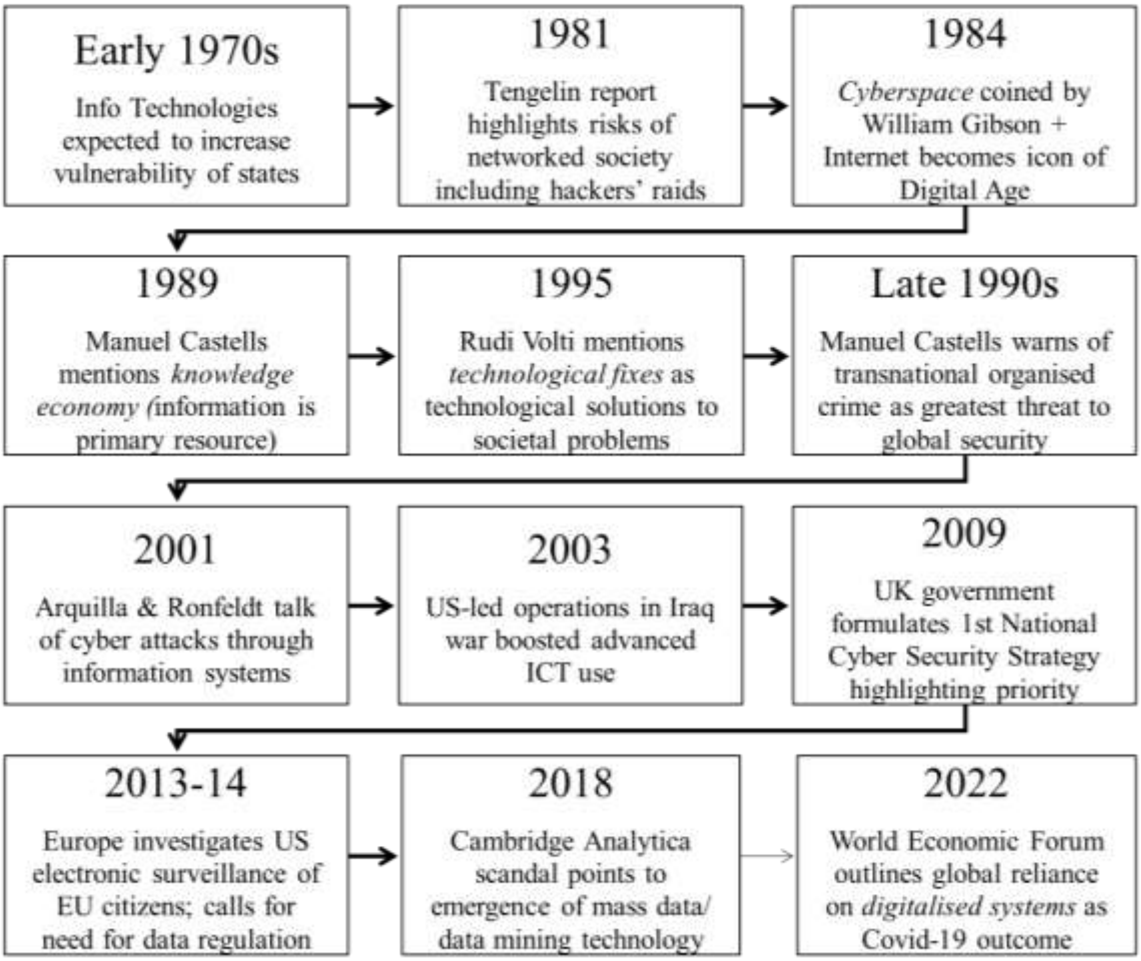
Early 1970s
Info Technologies expected to increase vulnerability of states
1981
Tengelin report highlights risks of networked society including hackers' raids
1984
Cyberspace coined by William Gibson + Internet becomes icon of Digital Age
1989
Manuel Castells mentions *knowledge economy* (information is primary resource)
1995
Rudi Volti mentions *technological fixes* as technological solutions to societal problems
Late 1990s
Manuel Castells warns of transnational organised crime as greatest threat to global security
2001
Arquilla & Ronfeldt talk of cyber attacks through information systems
2003
US-led operations in Iraq war boosted advanced ICT use
2009
UK government formulates 1st National Cyber Security Strategy highlighting priority
2013-14
Europe investigates US electronic surveillance of EU citizens; calls for need for data regulation
2018
Cambridge Analytica scandal points to emergence of mass data/ data mining technology
2022
World Economic Forum outlines global reliance on *digitalised systems* as Covid-19 outcome

Figure 2.2 Evolution of cybersecurity in literature. ***Source****: Developed further from Eriksson and Giacomello (2006)*

Another scholar, Hamid Mowlana, discussed the possibility of negative consequences of the growth of information technology, by pointing out the potential use of information as propaganda, in the late 1990s (Mowlana, 1997). This was further witnessed in the theory of Securitisation, developed by the Copenhagen school, which discussed possible perspectives on security concerns (Waever, 1995; Williams, 2003). Looking at this in the instance of Swedish politics, Eriksson (2001) was able to distinguish between government outlooks on responsibility allocated for IT-related threats. Cybercrime was labelled so when criminals were blamed for the event, while information warfare was the term of choice when it was used by a state to respond to an event of threat.

Around this time, Arquilla and Ronfeldt had expressed their concerns, which had gained wide acceptance, of the information revolution making security a growing concern for the society at large (Arquilla and Ronfeldt, 2001). In the new millennium, a war in the digital age (or digital war0 was observed to have some of its actors from the harsh or bloody realities of the war (Der Derian, 2000). Simulation (or virtuality) was another feature of this digital war, and hence every possible source of simulating threat events and responding to them, including film and cinema were popularised as an inspiration and expertise for the military (Der Derian, 2000; Everard, 2000). Thus, to address the issues associated with digital-age security concerns, symbolic politics (first developed by Murray Edelman) has been proposed (Eriksson and Giacomello, 2006) to varying degrees of success.

Since 2001, this term has been an integral component of contemporary vocabulary and no longer limited to futuristic discussions at forums and academic literature. Now, addressing the cybersecurity concerns of today and tomorrow is a field of increasing significance, and discussed in detail in 2.4.4. and 2.4.5, respectively. Thus, after having looked at the bigger picture of cyberspace, military, state, and society, we can appreciate its significance for organisations. Katz and Kahn (1978), point out the intellectual revolution that swept Organisation theory in the 1960s and brought in the view of organisations as open systems, with an underlying assumption of interdependency (Thompson 1967). An interesting perspective is thus to imagine how organisations would evolve in light of advancing technological innovations. Since technological innovations recombine elements of previous innovations (Kogut and Zander 1992), recombination may be considered an elementary component of the evolutionary process for organisations, from a cybersecurity perspective.

Between 2001 and 2003, US-led operations in Afghanistan and Iraq, respectively, boosted the employment of ICT at various levels of the war (Tikk-Ringas, 2015), highlighting an increased focus on ICT for war purposes. Over the next few years, this domain thus gained significance in political contexts, leading to the UK government drafting its first National Cyber Security Strategy in 2009 (Stevens and O’brien, 2019). Similarly, the need for data protection and regulation was highlighted within the European Union, when it authorised an investigation into the US government agency’s mass electronic surveillance of EU citizens in 2013-14 (Dobák, 2021). The emergence of digital data and its use led to increased concerns about the development of data-mining technologies and their deployment by organisations and/or nations. This was highlighted by the infamous Cambridge Analytica scandal (Hu, 2020). The Covid-19 pandemic further underscored the growing concerns regarding *digitalised systems* (World Economic Forum, 2022), experienced at a global level. This brings us to the state of cybersecurity in contemporary times, which is discussed in the next subsection.

2.4.4 Cybersecurity Today

In the world of today, the damages posed by cybersecurity breaches to an organisation's reputation (Kewell, 2007; De Minville, 2020; Gale, Bongiovanni and Slapnicar, 2022), financial standing and legal situation (Nolan, Lawyer, and Dodd, 2019), are relatively well-known. These are the primary reasons a firm would want to take measures to guard against potential cyber vulnerabilities, to their best abilities. However, another area that requires attention is the relative market loss that the cyber-victim organisation undergoes as rival firms may be able to gain from the former's cyber challenges, even when the cyber-attacks were not facilitated or sponsored by them. Competition in the market ensures that as one firm loses, another one gains. And this is why, the objectives and motivation (Brantly, 2014; Rai and Mandoria, 2019; Chng *et al.*, 2022) of cyber-attacks may not always be known. Any or all information-gaining, destructive or obstructive activities (Kiss, Breda and Muha, 2019) could be the goal behind such cyber campaigns conducted by state or private actors.

It is increasingly clear that, while failing to implement basic block and tackling practices has been equated with forgetting to lock the back door (Landefeld, Mejia and Handy, 2015), cybersecurity measures are not a measure of choice anymore. In recent years, there is no possibility to have avoided being made aware of a major cyber campaign against an organisation, as it gains immediate and wide public attention and interest. Large organisations with the potential for large losses most often cannot avoid mass attention when such events occur, but this does not mean that smaller-sized firms escape such attacks. Traditionally, security threats were less vicious, which could have been natural disasters, theft of hardware/ software, unauthorised access, or human error (Loch et al., 1992). However, in modern times, these have become more hostile and targeted as hacking and cyber terrorism (Furnell and Warren, 1999) or virus attacks (Post and Kagan, 2000). But the list of potential nefarious cyber activities is not limited to hacking and terrorism.

One way to approach cyberspace attacks could be to first identify the potential point of entry of the threats themselves. Since these breaches occur in the cyber realm of the victim's information and communication technologies, there are five potential sources of cyber vulnerabilities commonly used by cyber-criminals. These are (Finnemore and Hollis, 2016):

- proximity access – allowing an adversary to connect through to the victim's network or another way, enabling a connection

- remote access - hacking, which does not require connected access and can be perpetrated from anywhere across the internet
- insider access – through unwitting players fooled into sharing access or social engineering techniques like spearphishing (an adversary poses as a trusted party to induce them to introduce malware - e.g., through an email attachment - into the system)
- supply-chain access – built within the software or hardware back doors, during creation or servicing
- denial of access – (DDoS – distributed denial of service) essentially flooding the potential victim's website server, incapacitating its ability to respond and/or disabling it for others

Campaigns against an organisation's information and information systems have been growing in number, variety, and severity (Fulford and Doherty, 2003). Whether it was the industrial virus Stuxnet in 2010 (Trautman, 2017) that caused kinetic damage to Iran's Natanz uranium enrichment facility (Zetter, 2015), the Shamoon virus attack at Saudi Aramco in 2012 (Bronk and Tikk-Ringas, 2013), the Sony Pictures hack after the movie 'The Interview' was released in 2015 (Craig, Shackelford and Hiller, 2015), general indiscriminate attack on Wannacry (Fiore et al, 2023) or the targeted damage campaign through BadRabbit in 2017 (Alotaibi, Vassilakis, 2021), the list of infamous cyber-attacks is exhaustive. Perhaps the most worrying aspect of cyber-breaches is that a single individual may invade the resources of an entire organisation, debilitating its system and paralysing its processes for a variable amount of time. Furthermore, these hostile campaigns are gradually learning from past instances and developing into more malicious and detrimental attacks, worsening the potential damage and recovery possibilities each time.

The damage from cyber breaches is worth billions in currency, but losses are considered in four primary categories – losses of confidentiality, integrity, availability, and indirect loss (Finnemore and Hollis, 2016; Wessels *et al.*, 2021). While the attack and the breach can last anywhere between nanoseconds and years, it is estimated that, on an average, the adversary has access to the system for 205 days before being detected (Mandiant, 2015). Such cases bring to light the need to invest in resources which help build competences which are helpful against the above-mentioned campaigns. There is also a growing need to build capabilities to be able to develop (Kiss, Breda and Muha, 2019) such defences over time, rather than just purchase or employ them. When the defences are of a self-sustaining nature, there is hope for them to be adequate when the need arises.

Most governments of developed nations, where IT is characterised by advanced use and propagation, have bodies in place to safeguard individual entities and ensure processes are followed. Yet the US, recognised as an industrial and technological power, has also witnessed some of the most damaging cyber campaigns (Walters, 2015). Perhaps, that was one reason they incorporated strategic state bodies to ensure better management of the cyber realm – both at an individual as well as an organisational level. The Security and Exchange Commission (SEC) and the IT Governance Institute (IT Governance Institute, 2003) have been placed to supervise transactions in the cyber space. The Computer Security Incident Response Team (CSIRT) at an organisational level and the Forum of Incident Response and Security Teams (FIRST) - as a global association of CSIRTs (Eugen, 2018) - are other authorities in existence.

The incidences of breach and attack may be characteristically different, with different potential targets and objectives, but other parts of the world, including Europe, are not prominently safer from them. At the European level (Bejan, 2022), the European Network and Information Security Agency (ENISA) is the agency other geographical neighbours collaborate with for cybersecurity matters (Catteddu, Hogben, 2009). The European Union's General Data Protection Regulation (GDPR) (implemented on May 25th, 2018) mandates that companies conduct privacy risk-impact assessments to analyse the risk of data breaches, including steps to minimise risk (Kalinich, 2017). These organisations and protocols describe the impetus shown by the governments in the US and European regions.

Closer home in the UK, just like the corporate governance system in the UK resembles its counterpart in the US (Cheffins, 1999), so have the cybersecurity breach campaigns and their management. Here, the Ministry of Defence has several bodies assigned to this task. The Foreign and Commonwealth Office works through the International Cyber Policy Unit and the NATO (Ministry of Defence, 2013). While there is a Computer Emergency Response Team (CERT-UK) set up since 2014 (www.cert.gov.uk), which works alongside the Government Computer Emergency Response Team, there is also an alliance of 750 organisations in the Cyber Security Information Sharing Partnership (Cabinet Office, 2009).

Serious cybercrime threats are managed by the National Crime Agency (Segell, 2007) which has a legacy of organisations like the National Cyber Crime Unit (NCCU), the Police e-Crime

Unit and the Serious Organised Crime Agency (SOCA) (Bowling, Ross, 2006). Furthermore, there are nine Regional Organised Crime Units (ROCUs) with cybercrime units under each of them. There is also the Office of Cyber Security and Information Assurance (OCSIA) which advises the cabinet and the National Security Council (NSC) in the field of cybersecurity and information assurance (Levi, Williams, 2013) (HM Government, Office of Cybersecurity, and Information Assurance link). The bodies created to counter cyber-attacks and effectively manage them, reflect the state's stance on cybersecurity per se. The priority they have shown to the topic is demonstrated in their activities conducted to combat cyber-threats.

Clearly, the emphasis on approaching cybersecurity with the priority it deserves is not lost on either the private sector or the public sector. Governments, in coordination with private enterprises (McCarthy, 2018), as well as corporates within and among themselves, are taking increasing measures to safeguard themselves. Procedures, mechanisms, and bodies are in place to best manage perceived and potential threats within the cyber realm. However, since the entire field of cybersecurity is hard to manage and predict, and also owing to the novelty of each successive threat (Bejan, 2022), the structure of cybersecurity is evolutionary at best. It may have matured since it first came into prominence; every few years the rate of growth and progress within the field of technology is considerable (Kosutic and Pigni, 2020b), in one sense; however, it is also adequate in keeping with the rate and state of threats, in another. Certain actors who have already suffered breaches or their aftermath have learnt swift lessons; others are trying to learn without have to undergo damaging cyber campaigns.

2.4.5 Preparing for Cybersecurity Tomorrow

The information age has brought with it an unfathomable volume of opportunities; however, as with any opportunity, threats have arrived simultaneously as well. Cybersecurity has emerged as the most challenging problem today (Balitzer, 2016), partly because, as vital the as the internet currently is, the rules of cyberspace are not universally known (Finnemore and Hollis, 2016). This problem of cyber-threats, while may be a product of information technologies, is the subject of argument in viewing the solution in policymaking (Mulligan and Schneider, 2011). The state of affairs is such that the security of the cyber space is neither wholly a government responsibility nor entirely managed by the private-sector players. Since the internet is not owned by a single individual or enterprise, there can be no single entity – private or government – which can completely protect the entire IT global infrastructure (Chertoff, 2008). When cyber breaches happen in the private sector, business leaders call on their respective governments to do more, but they realise it is more of a corporate responsibility (Stoddart, 2016).

Within the private sector particularly, the threat of counter espionage and/ or sabotage enhanced by modern technologies is a valid concern. While discussing the future of cybersecurity, not considering this aspect would be amiss. Ranging from insider IT sabotage (Moore, Cappelli, Trzeciak, 2008) aimed at either sabotaging/ harming the organisation or individuals associated with it, to corporate espionage aimed at appropriation of information through improper means (Miller, 2000), private sector's cyber-vulnerabilities lay further exposed. Considering this information attempted to being exploited by organisations is now stored and maintained on cyber-assets or virtual clouds (Rothke, 2001), the threat is further enhanced by the cyber-vulnerabilities, which makes the threat two-fold. Counter espionage has implications for the individual stakeholders involved with the organization being highly controlled/ monitored (Chan, 2003) within organisational security measures.

The threat to organisations, brings to the fore the idea that a polycentric approach to addressing cyber-threats may be more realistic than an individual organisation or country-driven approach. Indeed, a multi-stakeholder model has gained popular support to be the dominant template for managing global internet governance (Carr, 2015) and to build the competence of systemic resilience (Stoddart, 2016). Using a coordinated approach at the organisational, regional, and global levels (Eugen, 2018) could be expected to bring more reliable and feasible solutions to problems which are affecting an increasingly larger number of organisations and states. (Broeders, 2016) talks of the growing need for widening the diplomatic arena for internet governance, including international governments along with private actors who even own large internet companies like Google, Apple, and Microsoft. He even proposed the idea of treating the internet as a neutral zone where no individual government may interfere to advance their respective interests. However, as novel as the notion may be, there cannot be any doubt over an increasing reliance on state structures to guide and lead the way for following cyber-related protocols and measures.

Indeed, a multi-party approach may be required to address cyber vulnerabilities at an organisational level, as the perpetrators could be any of the following four adversaries (Finnemore and Hollis, 2016):

- hackers – individuals with the potential to wreak havoc on another individual or at a commercial/state enterprise, with varying levels of motivation for the attack, ranging from proving the superiority of their skills to gaining a financial advantage or causing significant losses
- hacktivists – these are often collective groups who are trying to influence decision-making for certain causes they believe in concerning a country, government, ideology, or issue (eg. Anonymous is an infamous group (Bunt, 2016))
- organised criminals – these are organised within groups, with mostly extortionist motives towards achieving disproportionate financial gains internationally, often exploiting territorial cyber jurisdiction limits
- states – intelligence agencies of governments have been known to either themselves or through proxies, author exploits or attacks for a variety of objectives ranging from gathering data to eavesdropping on other governments, private enterprises, or individuals (Geers et al., 2014), even though scholars such as (Valeriano and Maness, 2018a) have found evidence to the contrary.

Gaining a better understanding of who the potential perpetrators of cyber breaches could be, is perhaps an encouraging first step to work towards mounting adequate cyber defences. Whether the adversary is an individual or a group, privately sponsored or commissioned by a state, motivated to gain financial benefits, or looking to become internet-famous (Thackray *et al.*, 2016; Rai and Mandoria, 2019), are all various facets of different cyber-criminals. Owing to diverse motivations and sponsorships, management of each would be varied as well. Some may be resolved privately while others may require support from state agencies, thus even exploring a possible public-private partnership (PPP) (Stevens, 2018) approach. This outlook focusses on private critical infrastructure ownership, supported by the state's promise of cybersecurity responsibility as a public good. Once having identified the probable adversaries, the organisations need to narrow down their approaches through which they choose to strategise for their cybersecurity management.

While discussing the implications of cybersecurity today, it is also essential to consider the impact of modern technologies synonymous with the 4.0 economy. Artificial Intelligence and Machine Learning are ordinarily considered useful for the functioning of modern organizations, allowing convenience, connectivity, and efficiency. However, these are also equally favoured by perpetrators of cybercrime, enabling automation and advancement of their criminal capabilities (Hoanca and Mock, 2020), thus allowing for an unprecedented increase in their capability, accessibility, and widespread deployment in recent times (Caldwell *et al.*, 2020). Whether it is identity theft, ransomware, or online fraud (Mishra, 2023), these technologies are being exploited to wreak havoc on individuals and organisations alike. The ease of use and unmatched range of functions allows even those criminals without technological expertise to abuse the capabilities provided by these technologies.

Some contemporary literature tends to focus on the reductionist approach to issues and challenges. In the case of cybersecurity, it amounts to focusing on specific cyber-attacks or cyber criminals to avoid future incidents, or solutions to individual problems as opposed to those of the entire realm (Gandhi, 2014). Rather than a reductionist lens, perhaps the need is to use a holistic perspective to better appreciate the challenges of today as well as pre-empt the potential problems of the future of cybersecurity more adequately. Such an integrated approach would align multiple perspectives – business objectives, governance, laws and regulations, economics, risk management, technology, psychology, and criminology (Tisdale, 2015).

The advantage of applying a holistic lens is that it is very much aligned with Complexity or Complex Leadership theory (Uhl-Bien, Marion and McKelvey, 2007) which, in turn, is particularly useful to strategise in the governance of cybersecurity issues. Scholars have identified the need to address the challenges posed by the 4.0 economy with the combined elements of soft skills, dialogue-based techniques (open and explicit risk discussion) (Kaplan and Mikes, 2012) and envisionment (scenario-planning) (Leonhardt and Wiedemann, 2015). Furthermore, they support a three-pronged approach to risk-governance for cybersecurity-related challenges: knowledge acquisition (gathering information to transform unknown to known risks), precaution approach (develop additional precautions for unknown risks) and fostering resilience (learning and preparing to cope with unexpected events) (Leonhardt and Wiedemann, 2015).

Scholars such as (Sallos *et al.*, 2019) also proposed a possible approach of going further and applying a strategic lens to the field. This would combine holism with other approaches like pragmatism (pragmatic approach), inference (adequate strategic inference of cybersecurity efforts) and adaptation (calibration based on feedback). They highlighted the need for an approach which is rigorously formulated and continuously adjusted, so as to make it most adequately applicable. Thus, the approach to cybersecurity, whether holistic or strategic or any other, would be subjectively dependent on the firm it is to be decided for. Cybersecurity for a small retail company, as opposed to a large financial enterprise, would have varying needs and outlook. However, the need for it to be evolving with time and developing resilience is constant with both approaches.

There are many other novel approaches to the field of cybersecurity, and academically investigating them could be the first step to understanding their possible effectiveness. As valid suggestions to expand the horizons of research into the field, these approaches are certainly worthy of being explored further. An interesting study was conducted to explore the association between the network services a particular computer node is hosting and the threats to which it is susceptible. This was done by drawing parallels in the field of epidemiology by drawing inspiration from the tools used in genetics to identify associations between mutations and diseases (Gil, Kott and Barabási, 2014). It is just an example of the kind of academic exploration being made into the field of cybersecurity to better assess potential models for finding solutions in algorithms and statistics. The problems of the internet are being sought, to be resolved by solutions on the computer.

Yet another fascinating perspective was to consider the field with a green lens, or an environmental approach. Scholars used another novel approach to better understand the relatively novel and dynamic field of cybersecurity to help manage it better. They posited that as sustainability in businesses was, at one point, a novel concept, so is cybersecurity today. It took Rachel Carson, a marine biologist's seminal book 'Silent Spring' to bring to focus the impact of pesticide usage, thus jumpstarting the modern environmental movement (Rachel Carson, 1962). However, since then organisations have increasingly accepted their responsibility in making sustainability an important consideration in their agendas. They integrated it successfully into their CSR (corporate social responsibility) initiatives, and its impact is palpable. By incorporating it into their CSR, companies can safeguard their customers as well as the public (Shackelford, Fort, and Charoen, 2016) in any number of possible ways; hence, proposing a similar treatment for how cybersecurity must be managed today.

A stimulating paper by Lango (2013) explored competing academic approaches to cybersecurity, which seeks quantification and analysis in context. Indeed, further investigations are required to better understand this dynamic field, where threats and breaches are perhaps evolving as fast as, if not faster, than the cybersecurity strategies that private enterprises, supported by the state, are employing to address them. While there is a great requirement for technological expertise to dominate the field, there are increasing voices supporting an involvement of the social science sphere imbuing itself to address the realm with more practically applicable solutions. Social scientists who code data, in association with practitioners who experience events, and policy makers who transform the data into actionable events (Valeriano and Maness, 2018b), are the need of the hour to approach this field and bring the balance of power back in the domain of keeping cyber space secure.

2.4.6 Cybersecurity as an implement of Corporate Strategy

Understanding an organisation is elementary to approaching the dynamic challenge that is cybersecurity. Relevant perspectives for this are open systems and complexity views. Open systems are those which exchange resources with the environment, and complex structures are those which have interdependent parts (Thompson, 1967). Modern organisations fulfil both these requirements; hence applying these perspectives to an organisation's strategic direction helps produce dynamic and self-organised solutions. To affect strategic organisational changes that evolve temporary advantage more rapidly over the competitors (Brown and Eisenhardt, 1998) would be to find their unique competitive advantage, which is the foundation for organisational success.

Viewing firms from the above approaches is useful in many ways, especially in the case of deciding their IT and cybersecurity arrangements. It has been found that the greater the relative importance of IT to the firm's ongoing operations, the greater the risk potential it faces (Parent and Reich, 2009). The elementary question, then, is – how does it prepare for cybersecurity in a fast-changing environment where, so little is known, and threats are novel? The answer lies in taking a top-down approach wherein the focus of deciding and preparing lies with the governing board. It has to approach cybersecurity as part of its risk oversight function, providing effective governance over information technology (Trautman and Alternbaumer-Price, 2011). However, there is no one-size-fits-all scenario for this field where cybersecurity needs are highly subjective to each firm, and therein lies their approach to it.

An international report on organisational approach to cybersecurity (Accenture, 2010) reported that most of the data breaches or losses were believed to be caused by the lack of internal controls and processes, and not hackers or viruses. Hence, the focus on managing IT-related risks rests on the able shoulders of a board, as Nader (1984) pointed out that boards cannot only rely on their confidence in the management. This begins with recognising IT as a core asset of firms. In today's 4.0 economy, it needs to be especially protected and managed as it supports and sustains entire organisations (Trautman and Alternbaumer-Price, 2011). Klinke and Renn (2006) recommend a three-step process to manage systemic risks – identify risk classes, create evaluation criteria, and design management strategies.

Corporate governance represents the area for achieving the company's goals (Eugen, 2018). Within this, adopting Filatotchev's (2007) perspective of boards, arising from the Agency theory, allows for taking one of the two forms of the directors' responsibilities. One is the defensive approach, which involves protecting wealth and, in the context of IT, could be considered as IT risk-governance. The other could be a more aggressive stance, aimed at creating wealth and, potentially, IT value-governance (Parent and Reich, 2009). This offers a great degree of clarity in deciding which form is to be adopted in a given firm, depending on its IT intensity as well as risk appetite (Leech and Hanlon, 2017). It is important to note that despite other roles and functions that claim their attention, board members need to be acutely aware of the sophisticated demands that cybersecurity issues will make of them, thus allocating time and resources toward IT accordingly.

Corporate oversight allows boards to pre-empt the risk associated with cybersecurity (Trautman and Alternbaumer-Price, 2011) and strategise accordingly. Since they have the required resources available to make informed strategic choices, perhaps they evaluate the scope of board review and then allocate the resources in making necessary inquiries from the management team. Over the course of time, the board may be expected to have perfected a customised evolved process to evaluate and address cybersecurity-related risks and solutions (Landefeld, Mejia and Handy, 2015). In the absence of absolute certainty (which may never be a feasible reality in this field) and perfect solutions, the above may be the most practically reliable solution available to corporations. Other policymakers could even replicate this, even at a state level.

This application would not only be applicable but particularly useful in the case of IT as a source of risk. Further, for any board to be able to govern it as an asset, the domain issues need to be adequately represented in the boards for them to be able to allocate the requisite attention and resources to them. *Parkerian hexad* (Parker, 1998) - which is comprised of confidentiality, integrity, availability, possession or control, authenticity, and utility - offers a model of required features of a security system to guide IT policies in an organisation. Taking cues from the above, and depending upon the unique requirements of the firm, the board could create risk committees, ensure necessary insurance coverage, and formulate crisis-management plans to better manage risks of the cyber realm. Having said that, there is a need for cybersecurity risk awareness to be at all organisational levels (Kure, Islam and Razzaque, 2018), where individuals follow protocols to safeguard their assets collectively. While the approach may flow from the board, cybersecurity measures can only succeed in conjunction with the combined efforts of the staff.

In the age of interconnected devices, IoT and AI, maintaining privacy is a huge challenge, which is where the potential for exposed cyber vulnerabilities comes into play. As long as information is stored on a connected device, keeping it completely secure is a challenge, which gets magnified once the information needs to be shared with another party. Classified information, confidential data and sensitive details could all potentially benefit from having reliably controlled physical spaces (Barnes, 2019) to be transferred using secure communication. Is there then an area of interest for the creation of such areas where companies could transact with otherwise-unprotected information (Kiss, Breda and Muha, 2019). Such self-sustained and safeguarded areas could be particularly useful for conducting negotiations, conciliations or other similar context-sensitive or classified information. For organisations, a successful response to the above situation could certainly be an investment worth making for all the reputational, legal, and financial costs (Nolan, Lawyer, and Dodd, 2019; Gale, Bongiovanni and Slapnicar, 2022) it would save.

In the US, the Securities and Exchange Commission (SEC) has outlined the need for public companies to disclose cybersecurity risks, along with provisions made for cybersecurity or privacy insurance. Further, public firms are also required to report cyber incidents that have taken place, as well as any material litigation regarding cyber incidents in their public reports **(**Li et al., 2018). The reason to mention such measures is also to bring to attention two features. The first is that the US example tends to be followed the world over, since the days of it having adopted the broader corporate governance construct in the 1970s (as discussed in 2.2.2.). And the second is that it reaffirms the need to take the focus of cybersecurity away from the individual and toward the collective (Mulligan and Schneider, 2011); thus, a polycentric issue as discussed in 2.4.5.

Viewing organisations from the point of view of the Complexity Theory as Complex Adaptive Systems (CASs) (Anderson, 1999) (discussed further in 2.6.1.7) also has certain potential benefits. Kauffman (1995) points out that all CASs evolve to the edge of chaos, as this offers them a selective advantage, which is evidenced in successful organisations as they strategically function at the edge of chaos. To achieve strategic equilibrium, they consistently make minor changes which occasionally cumulate to radical strategic innovations, setting them apart from their competition, as argued by Brown and Eisenhardt (1998). Cybersecurity and its management are a fine example of this path to strategic equilibrium, whereby organisations can achieve competitive advantage by the investment they make in it.

Digital advances, while having created potential risks, have also created opportunities for growth and success. The governing board, along with its executive team, has to determine if the competitive advantages are being created from these opportunities, while simultaneously dealing with the risks (Grove and Clouse, 2017). Scholars have reaffirmed the importance of board engagement in the enterprise's planning for its business technology governance (Masli et al., 2011). Since business technologies are integral to how businesses operate (Valentine and Stewart, 2013), boards need to acknowledge the need to prepare for IT as a resource at the board-level, instead of delegating it. Firms need to invest in their information or business technologies on the basis of their perception of risks (Grant *et al.*, 2014) – competitive, financial, and reputational (Valentine and Stewart, 2013). Only then, can issues of prime significance like cybersecurity may find appropriate solutions.

Thus, there is a need to recognise cybersecurity management to have the ability for a rigorous formulation, and for it to be continually adjusted (Abraham and Sims, 2021) so as to yield a contextually satisfactory result (Sallos *et al.*, 2019). Just as workplace safety and security measures are part of the business culture, so do cybersecurity best practices (Stoddart, 2016) need to be ingrained in the normal course of business. Innovations, hiring the right personnel (Nodeland, Belshaw and Saber, 2019) (including at the board level), pre-empting threats, and treating cybersecurity as an investment into the organisation's safety and future, allow them to be successful.

2.4.7 How Significant is Cybersecurity?

It is widely accepted that information is a key corporate asset and, thus, of great commercial value (Gerber et al., 2001), and hence information security is at the top of the agenda (Fulford and Doherty, 2003), as explored in the previous section. However, to decide whether cybersecurity is indeed the answer, what the question is must be known. If it is to decide and support the survival of the business, then a dedicated outline of cybersecurity may not even be needed. In contrast, for firms contemplating their approach to cybersecurity, survival should not be the goal (Grove and Clouse, 2017) but, understandably, the necessary first step. If the question is to find a unique sustainable advantage in the digitalised 4.0 economy, which will not only allow survival but potential business success, then perhaps the answer may be unlocked in the cybersecurity domain.

At the World Economic Forum at Davos, Switzerland in 2016, 735 board members and executives voted for speed of disruptive innovation as the fourth highest risk for business in 2017 (Amato, 2016). Here, *Industry 4.0* came to influence and change the scene for the cyber realm forever, thus increasing the reliance on 4.0 economy technologies like Big Data, Artificial Intelligence, Internet of Things, Neural Networks and Deep Learning (Cristea, 2020). When such modern technologies are being increasingly used for the day-to-day functioning of businesses, their pitfalls and vulnerabilities need to be better managed. If we consider three levels of requirements – necessities, comforts, and luxuries – where the first represents absolute requirement and progressively decreases in degree with the next level, cybersecurity cannot be considered a luxury either now or in the potential future. As enterprises lie more exposed to novel and unprecedented threats in the cyber realm, preparing for a fortified security program and processes will have to be a necessity.

Furthermore, contemporary organisations rely on virtual working, where not all employees work at their desks; some simply work from home, or on the go (Hutchins, Britt, 2020). Such ease is provided through the comfort offered from Cloud which facilitates not only computing, but also storage and security measures for businesses. Such instances are not exclusive cases, but increasingly becoming the norm, which further necessitates a strong and reliant cybersecurity management system (Malecki, 2020). Hiring an IT manager with excellent skills will not be adequate in such times when IT and cyber realms need a dedicated voice at the governing board and top-management team levels.

In medium and large corporations, which have found comfort in their traditions and existing methods, the transition to such advanced cybersecurity reliance may be a challenge on its own. While adoption, management and reliance on technologies are on one side of the coin, familiarity and comfort with those technologies are on the other. Heimer and Valeur (2016) mention the non-profit organisation Board Apprentice which places digital apprentices at boards for a year's duration, which further helps educate both apprentices and boards in five countries. Perhaps, this could be one way of approaching this new shift companies need to adapt to. Bringing in a new era for cybersecurity governance (Eugen, 2018), cybersecurity is, thus, a vital part of corporate governance of today and tomorrow.

2.4.8 Summary of Cybersecurity

In the contemporary times of digitalisation, cybersecurity risks are magnified owing to recent technology trends (Grove and Clouse, 2017) like Big Data, AI and IoT (Cristea, 2020). As the risks have increased, so have more vulnerabilities been exposed, which significantly increases the need for an adequately assertive approach to cybersecurity. Since the cyber space does not have boundaries, it cannot even be controlled by an individual government or private-sector actor. Hence, the need for a combined polycentric treatment of challenges posed by cybersecurity. Private enterprises or the state authorities alone cannot safeguard themselves and the associated customers and public, respectively, from cyber-breaches. Scholars, public, practitioners and policymakers ought to work in tandem to discover apt solutions.

As the threat of cyber-attacks looms large on organisations, big or small, the only possible course of action is to prepare for it. Firms today need to elevate cybersecurity on their agenda (Posthumus, Von Solms and King, 2010) including, not just board intervention, but complete board involvement to strategise a fitting approach for cybersecurity. Whether it is employing an expert or allocating a committee, the board is urgently required to set the policies and processes in place. These measures, in turn, need to be followed throughout the company. Overall, cybersecurity, and the attention it deserves today, is not a matter of choice anymore - it is a question of survival and possible long-term success. As is famously attributed to Charles Darwin, within species it is often the one that is most adaptable to change that has the most chances of surviving (Darwin, 1909). In that respect, it is a matter of evolution for the digital enterprise or digital-reliant organisation of today and tomorrow. Thus, this section enables an appreciation of cybersecurity as a critical element for organizations which hope to not only survive but thrive amidst tough competition and malicious cyber-criminals.

2.5 Research Gap

The above review of literature covers the advances made in the three main fields this research is based on, namely – boards and corporate governance, strategising for competitive advantage, and cybersecurity. The extant literature has conducted several explorations into individual subjects from amongst the above three areas. Boards within the realm of corporate governance have been a popular subject area for both scholars and practitioners to explore their inner workings, motivations, theoretical frameworks, purpose, role, and contributions. Similarly, major leaps have been made in the cumulative literature that discusses, albeit with different perspectives, the board’s influence on its strategic role. How strategies are drafted today, and what influences a firm's choice for its competitive advantage, are also relatively well covered through academic and practitioner literature. Finally, the novel world of cybersecurity and the growing and potentially unpredictable world of cyber-*insecurity* are also witnessing studies across the globe.

2.5.1 Research Opportunity

In today's 4.0 economy, how is it that a board approaching the issue of cybersecurity and preparing for the firm's specific model of competitive advantage - that can sustain the test of time and survivability - is an area worth exploring? Cyber breaches are considered significant threats to an organisation; this research intends to help organisations not only ably defend themselves against these cyber-threats but also derive advantages over their rivals through cyber-defence. Such an enterprise carries on its shoulders a substantial responsibility as it could possibly lead the way for a new perspective in approaching the issue of organisational cybersecurity. By attempting to create a new framework of utilising cybersecurity governance (Ferrillo, 2014; Maleh, Sahid and Belaissaoui, 2021) as an organisation's competitive advantage, this study intends to help organisations throw light on the very private world of the board's involvement in strategy-making and the executive team's role in drafting and implementing that strategy.

The FT and Chartered Governance Institute Boardroom Bellwether 2022 survey of FTSE 350 companies highlighted that cyber-risk is amongst the top three factors contributing to increased risk (Chartered Governance Institute, 2022). Hence, practitioner reports mirror the increasing relevance of a study of this nature, aimed at developing strategic perspectives which would enable the designing and building of robust corporate cybersecurity mechanisms. While it may be surmised that, with changing times, cybersecurity is a crucial strategic issue of governance, understandably, knowledge such as this may not have been sought before.

Furthermore, this research explores the current positioning of cybersecurity within a cross-section of corporates and their processes to tackle its associated threats and opportunities. Enhancing competitive advantage through augmenting differentiation, while simultaneously minimising risk in a cyber-enabled world, could be imperative lessons for practitioner literature. Owing to the recent nature of digitalisation, strategising for cybersecurity and its role in governance is not optimally developed. This allows for its potential influence and impact on the future themes of governance, such as reputation and competitive edge.

2.5.2 Research Question

Changes in the global technological landscape have led to how information is exchanged and used – without borders, virtually, continuously, and autonomously (Haleem *et al.*, 2022). Even organisations which are not in the domain of technology are forced to acquiesce in the reality of progressively dealing with novel and menacing cyber-campaigns. Unlike other challenges which may interrupt the ordinary course of business, this problem is impossible to absolutely prevent and extremely difficult to accurately prepare for. Hence, cybersecurity is an increasingly topical issue for organisations internationally, and becoming a vital component of their strategic planning.

The goal is to explore the possibility of corporate governance moving to an era of cybersecurity governance (Eugen, 2018). However, the question still remains as to how does it figure on the strategic role of the boards? Is it to be encompassed under risk to be guarded against, weakness to be fortified towards, challenge to be overcome, or potential strength to be identified and prepared for? Is there potential for governing boards, in conjunction with their executive teams, to adopt a proactive stance in addressing this challenge, in order to derive competitive advantage from it? This brings us to the research question this study wishes to answer.

- *How do board directors consider and position cybersecurity as a critical element of corporate strategy in order to realise competitive advantage?*

2.6 Theoretical Foundation

Having explored the three main pillars of this research, and identified the research question arising from those, this section now explores the significant theoretical influences for this study. Literature has provided context for various theories which have been considered here. However, from amongst them all, one theory has emerged most prominent to function as the guiding theory for this research: Stewardship theory (Donaldson, 1990). Together, these nine theories are discussed in the following section:

2.6.1 Considered Theories

With the discussion of the three primary areas of this research, literature has brought to the fore a few theories which resonate with this fascinating field of research. These theories, in several ways, also influence the research - supporting its progress and development towards understanding this subject matter. However, through the process of examining these theories, it became evident that, despite their merits, they do not create the foundation for developing this research. Moreover, examining them enabled the clarity to identify the theory most suitable in guiding this study. These theories are discussed next.

2.6.1.1 Resource-Based View

Resource-Based View and Resource Dependency theory are both theories in strategic management, which are linked by their reliance on resources. However, this is where the commonalities end. Resource-Based view, while having been first proposed in the 80s (Rumelt, 1984; Wernerfelt, 1984), has been the dominant theory in the field of strategic management, helping firms identify the attributes of their resources and capabilities which could be potential sources of sustained competitive advantage (Barney and Clark, 2007c). Strategising for achieving competitive advantage, especially, brings to focus the Resource-Based View, which analyses the conditions under which corporate governance can be a source of sustained competitive advantage (Barney, Wright and Ketchen, 2001). The ability to use IT to leverage fundamental resource-led competitive benefits enables IT to be a potential source of sustainable competitive advantage (Mata, Fuerst and Barney, 1995). This is of particular importance when treating cybersecurity measures as part of IT or the larger umbrella of information systems including IT, and understanding the capabilities derived from it (Hulland and Wade, 2004).

This framework provides background to answering how successful firms strategise competitive advantage, especially from the resource perspective (as opposed to a product one (Wernerfelt, 1984)), which is an integral element of this research. Interestingly, in this view, some scholars advocate that the term *resources* was meant to largely encompass other popular terms such as knowledge, assets, capabilities, and dynamic capabilities, depending on which of them was being used as the independent variable. However, (Priem and Butler, 2001) argue that this inclusive definition of resources leads to difficulty in establishing contextual and prescriptive boundaries. For the purpose of this research, this inclusive view is certainly helpful as cybersecurity is a novel subject which may not be considered a category of its own and is best construed as an element of information technology or information systems (Hulland and Wade, 2004).

There have also been different opinions as to the definitions, and what they entailed within the view. For instance, some scholars have suggested that competitive advantage, on its own, be decided contingent on two factors – endogenous ones like resources and capabilities, and exogenous ones like the firm’s position in the industry (Huang *et al.*, 2015). This is relevant for this study in particular, as while the cybersecurity-led opportunities are being explored, they are being considered within the larger context of the industry sector and the era of digitalisation, as well.

Other academics have viewed that the initial version of the theory was limited in its application to corporate strategy, while being adaptable for competitive strategy only (Bowman and Ambrosini, 2003). They extended the idea of replacing resources with dynamic capabilities, which referred to a firm's ability to alter the resource base by creating, integrating, recombining, and releasing resources (Eisenhardt and Martin, 2000), which would allow its applicability in business strategy. This is a fascinating aspect to explore for this ever-evolving domain, where the exact categorisation of the asset within a resource or capability is not being called into question. The important perspective is to explore its association with the potential to enable competitive opportunities for the organisation. Accepting the resources as core resources and capabilities as dynamic resources (Hulland and Wade, 2004) may be one way of side-stepping the concern.

Being able to identify the correct set of critical resources for a firm (the VRIO resources mentioned in RBV (Barney, 1991)), and the proportion of investment needed in them cannot be pre-decided by a formula or even a theory. These are delicate subjective issues, which all organisations have to decide for themselves over time. Similarly, in the context of cybersecurity capabilities of the firm, abundant expertise and real-world experience are key factors in decision-making. Thus, while the process of identifying the strategic assets may be simpler, being able to develop them to their full value (Peteraf, 1993), requires further investigation and study. Thus, for this research, this theory holds significance as it allows an investigation into the specifics of the elements, which allows it to use cybersecurity in order to derive competitive advantage from it.

2.6.1.2 Role Theory

The importance of *role* as a sociological concept has been evident since the 1920s and Ralph Turner (1962), in his seminal work, discussed the importance of roles in understanding the cluster of individual behaviours, including in workplace settings like organisations. It originated from two separate theories in social psychology – Structural Theory and Symbolic Interactionism. From the former perspective, the earlier interpretation of role was in the form of performance of duties and obligations associated with the position or status of each role, wherein the underlying assumption was of individuals as conformists, who did not deviate from their socially-accepted roles (Martin and Wilson, 2005). From the latter perspective Biddle

(1986), highlights the interpretation of the role as a consequence of development from social interactions. Both these perspectives underscore the pertinence of roles in the context of cybersecurity. Expertise in IT, cybersecurity and crisis-management are factors which enable appropriate decisions regarding cybersecurity strategy. However, whether these skill sets are objective assumptions or evolved expectations from governing boards is a useful perspective for this study.

Roles are known to be more dynamic within organisational context than within other social structures (Sluss, Dick and Thompson, 2013). Therefore, any changes in organisational factors inherently lead to changes in role identities, as viewed by individuals in the given organisations. So, an organisation going through a merger or acquisition or undergoing technological recalibration, may very well affect the way managers assess their roles and performances within those. In such circumstances, roles would need to be adjusted through *role modification*, (Wrzesniewski and Dutton, 2001) with a view to enhance outcomes in performance. This is of particular importance to this research as the field of technology is constantly evolving (Kosutic and Pigni, 2020b), which further necessitates the role-modification of those involved in crafting cybersecurity strategy.

Roles form the basis, not just for individuals but also organisations, through structured interdependencies and intertwining tasks and responsibilities (Biddle, 1986; Katz and Kahn, 1978; Stryker and Burke, 2000). Thus, the roles of the organisational leadership co-exist with those of the governing boards, further impacting the decisions surrounding cybersecurity choices. Furthermore, board members perform multiple functions within their roles – for instance, performance-role as well as conformance-role (Tricker, 1994). This provides context for the skill set expected from contemporary board directors. While they may not be expected to have particular expertise in IT and cybersecurity (Hartmann and Carmenate, 2021; Gale, Bongiovanni and Slapnicar, 2022), they are expected to be cyber-aware in order to scrutinise the strategic choices of cybersecurity adequately (Cerin, 2020).

Finally, governing boards of organisations, understandably, have tremendous pressures to contribute to varied aspects of their firms' survival as well as success. Viewing the various aspects of such roles – consensus, conformity, role conflict/resolution and role taking – aid our appreciation of the varying levels of success which these board members have achieved in their roles. In the digitalised context of the 4.0 economy, with evolving cyber and other risks, the roles of boards are increasingly expected to evolve simultaneously (Landefeld *et al.*, 2017). To view their roles as an evolution from their earlier elementary requirements allows us to find a theoretical foundation in their contemporary deliverables, thus providing relevance and context for this research.

2.6.1.3 Agency Theory

The Agency Theory (Jensen and Meckling, 1976) has long been considered the dominant theory in the field of corporate governance, with its impact being evident in the creation of contemporary governance codes primarily following it or as the implicit theoretical background (Cuomo, Mallin and Zattoni, 2016). Fama and Jensen (1983) highlighted the need for adequate monitoring mechanisms to be put in place which would protect shareholders from the management's conflict of interest (agency costs). Within the context of cybersecurity, it is important to note that several organisations' chosen stance for cybersecurity is from a risk-compliance perspective (Landefeld, Mejia and Handy, 2015; Batra, 2020) which is mirrored in this theory. The premise of this research proposes exploring beyond a compliance perspective, yet considering this control mechanism of compliance is essential to support this study.

As far as the strategic direction of the firm is concerned, scholars over time have argued different interpretations of the theory. Some, like Zahra and Pearce (1990), acknowledge this perspective puts an impetus on the board to articulate the firm's mission, as well as the development of strategy and its implementation. As such, control as a mechanism can shape the strategic direction of the organisation (Stiles and Taylor 2001), which is vital to a firm choosing its competitive advantage from among its characteristic features and resources. However, views such as those of (McNulty and Pettigrew, 1999) insist that strategy development is an iterative process, elements of which would reside in the control view of the Agency Theory (Jensen and Meckling, 1976), and others in the Resource Dependence perspective, as directors draw upon their experience (Hendry and Kiel, 2004) and networks.

An enterprise deciding its strategic policy with respect to cybersecurity presupposes the adherence to monitoring duties which, in most firms, is the reason risk-compliance is followed. Since, cybersecurity also often is a component of this measure, the control perspective pioneered by the Agency Theory (Jensen and Meckling, 1976) cannot be diminished. However, this research is based on the foundational understanding that using cybersecurity to strengthen an organisation's competitive position cannot be followed from merely pursuing a compliance requirement. When a firm wants to rely on cybersecurity strengths as their unique advantage over competitors, other theoretical perspectives, such as stewardship and resource-considerations (discussed above), gain priority. Hence, while this theory may be the foundation for cybersecurity management, it is in want of further theoretical support in the context of cybersecurity governance.

2.6.1.4 Real Options Theory

Decision-making in uncertainty, as a topic, has been popular with scholars over time as it allows the investigation and development of theoretical frameworks which would address the issues highlighted by uncertainty. The Real Options View, introduced in the 1980s (Bowman and Hurry, 1993), supports a theoretical perspective which may guide the path of strategy-making in the midst of uncertainties. Especially, the 4.0 economy and its enabling technologies witness an evolving digital landscape, which brings forth uncertainties like cybersecurity threats and vulnerabilities. In this context, exploring the decision-making for a 'moving target' (Landefeld *et al.*, 2017), such as cybersecurity, may be supported by a theoretical framework such as this.

Building on the foundation of rationality, while keeping options open during times of uncertainty, would offer inherent advantage when applied to organisations (McGrath, Ferrier and Mendelow, 2004). This premise offers a unique perspective on strategy-making during uncertain times, which could hold significance for any study attempting to explore the strategy surrounding cybersecurity planning. In literature, viewing options as a strategy heuristic has been proposed for developing important capabilities and business portfolios (Courtney, Kirkland, and Viguerie, 1997; McGrath and MacMillan, 2000). If cybersecurity measures were to be seen as business-capability options, this could be considered helpful in crafting the necessary strategy around them.

A complication develops, however, when we delve into details of what could be considered the influences of uncertainty. Primarily considered either endogenous to a firm or exogenous forces outside a firm's influence (Majd and Pindyck, 1987; Roberts and Weitzman, 1981), this factor categorisation helps appreciate the challenge and find a solution to it. Technical uncertainty, from an endogenous perspective at the hands of the firm, would allow two options – to preserve the option of investing in it, or to abandon it in the face of exogenous shocks (Folta, 1998). Contemporary organisations, however, may not find the requisite answer to the challenge with such binary approaches. This is a limiting view of uncertainty and its factors, as options are ordinarily more complicated than this binary approach. Cybersecurity strategy, similarly, requires iterative planning and scrutinising to decide the most appropriate mechanism for an organisation.

Thus, the simplistic nature of this theory is perhaps also the drawback, in that it does not allow for a complex issue, such as deciding the strategic course of action to position cybersecurity as a competitive advantage, adequate theoretical support. Hence, the need to perhaps develop a new theoretical framework which would further build on the learning drawn from the Real Options theory and pave the way for firms strategising in this uncertain and dynamic arena. For this research, while this theory offers elementary support, there is a need to explore further for more and other theoretical influences.

2.6.1.5 International Relations Theory

Originating with (Arquilla and Ronfeldt, 1997)'s concept of CyberWar, information technology advances have provoked fear globally. Applying this theory for analysing the information revolution may lead to insightful understanding of the impact of cybersecurity (Eriksson and Giacomello, 2006). Using the *Island of Theory* approach promoted by Guetzkow (1950), collaboration may be understood to be the cornerstone of success in the cybersecurity domain. The International Relations Theory thus rests on the assumption of digital interconnectedness (Corallo, Lazoi and Lezzi, 2020), which leads to the understanding that potential vulnerabilities of individual states/organisations may not be faced single-handedly.

Many modern theorists have focused their attention on security studies, as a subsection of the International Relations Theory, to address the heightened fears of increased vulnerability arising out of the transition from *industrial* to *information societies* (Alberts, 1996; Henry and Peartree, 1998). While the situation may not always be as dramatic as cyberwar (Arquilla and Ronfeldt, 1997; Danyk, Maliarchuk and Briggs, 2017), there is a real threat as boundaries have merged between international and domestic, civil, and military, and private and public. This implies that not only information systems, but the organisations employing them lie vulnerable to these cyber-threats.

Defence vulnerability is also found to be highly correlated to advanced industrialised societies (Valeriano and Maness, 2018b). This highlights that increased cyber connectivity, in turn, leads to potential vulnerabilities and, hence, more is at stake. Thus, accepting increased cyber-vulnerabilities of organisations would inherently encompass peering across the jurisdictional borders to explore solutions. Finally, this theory acts as a useful steppingstone to further explore this intriguing domain eventually leading to development of more appropriate theories, especially created for the field.

2.6.1.6 Stakeholder Theory

Freeman, 1984, through the Stakeholder theory, introduced the coordinating role of boards of companies, wherein they oversee the interests of all the groups in society to whom the corporation is responsible - its stakeholders. Broadening the scope of the firm beyond the fulfilment of financial objectives, this theory found resonance in considerable empirical research which highlighted the notion that the firm can and should serve the interests of multiple stakeholders (Preston and Sapienza, 1990). This is particularly of significance for the domain of organisational cybersecurity strategy, as cyber-assets often comprise valuable multiple stakeholder information (Hubbard *et al.*, 2021). Thus, exploring adequate mechanisms to protect that information may find its theoretical foundation in theories such as this.

In the contemporary 4.0 economy, value creation and maintenance are high on the priority list of strategists. Additionally, with growing concerns of capitalism and the lack of ethics in consideration, a stakeholder approach could prove to be a potentially helpful approach. Also, from a strategy-making point of view, this theory is certainly useful in clarifying the objectives as well as for whom the strategy is being crafted. Furthermore, this theory has found applications in disciplines like law, healthcare, public administration, environmental policy, and ethics (Freeman, Harrison, Wicks, Parmar, and de Colle, 2010). This is helpful, considering a host of several diverse industry sectors would benefit from such theoretical leaning.

A modern firm’s customers, employees, sellers, resource-providers, consultants, and general public are vital stakeholders. However, from a simple corporate governance perspective, the inherent issue with this approach is the inability of addressing the divergent interests of the various parties involved, as well as creating a hierarchy of actions in response to them (Bonnafous-Boucher and Porcher, 2010). However, when we consider the domain of cyberspace, and the increasingly novel breaches and campaigns that can potentially attack firms, the Stakeholder Theory is not adequate to address all the concerns. Therefore, we need to look at certain other theoretical influences to explore a better fit in terms of an existing theoretical framework.

2.6.1.7 Complexity Theory

Another theoretical influence would be from the Complexity theory (Waldrop, 1993), which was borne of the Systems Theory. Largely inspired by biological systems with multiple applications, this perspective looks at analysing complex systems which constantly change to gain insights on strategic management with a focus on continuous adaptation. Considering modern organisations as examples of complex adaptive systems (Anderson, 1999), this theory acts as a guide to prepare for uncertain cyber environments, including cybersecurity threats.

Proponents of the theory highlight that computer software is inextricably linked to complexity, as that is one of the reasons why we depend on computers – to conduct complex functions (Wolfram, 2002). However, this is also bound to the unpredictability of information systems. This is because computers are capable of unforeseen emergent behaviour (Kauffman, 1993), of which vulnerabilities could be one kind (Armstrong and Mayo, 2009). Such studies point to the potential of using this theory towards approaching the challenges of cybersecurity from a quantitative perspective, the algorithmic nature of which has the potential to address at least some of the issues of the field.

In the case of organisations, managers are mostly trained under conditions of certainty, where they are now exposed to complexity, uncertainty and turbulence which might lead to other theories in the field such as the Complexity Leadership theory (Uhl-Bien, Marion and McKelvey, 2007). Hence, they need to balance between structure and continuous change through flexibility and adaptability, which emerges from a complexity perspective (Mason, 2007). Overall, we may surmise that the Complexity Theory, despite its origins in the twentieth century, lays down a reasonable foundational approach to twenty-first century topics like cybersecurity. However, while this theory provides the general background for a study about how organisations can strategise for areas as dynamic as cybersecurity, it fails to support the possibility of an enterprise broaching this challenge from a strategic competitive advantage perspective. Theoretical support that encompasses both these areas is required and currently lacking; thus, the need to continue investigations to render such a framework.

2.6.1.8 Contingency Theory

While discussing a company’s strategy, it is not possible to move forward without discussing the several factors which affect it. These contingency factors are in the form of both specific characteristics of the organisation as well as the nature of its environment, which have an impact on the organisation and its structure, (Steiner, 1979). Thus, in the absence of a good universal structure that can be adapted to all situations, a good structure for a company would be one which is adapted to the environment (Enjolras, Camargo and Schmitt, 2019). The Contingency Theory reasserts the importance of basic economic and technological forces (Hofer, 1975) at play, in corporate strategy. Hence, when the economic scenario changes or when an important stage of the product life cycle is reached, it may be time to re-evaluate strategy, according to this approach.

This becomes especially useful to consider with respect to contemporary technological advancements which render previous technologies obsolete (Kosutic and Pigni, 2020a), which have a considerable impact on all businesses. Thus, being an extension of the technological paradigm, perhaps cybersecurity would require a consideration of contingency factors. Regulatory climate, external risks from criminals and the growing scope and complexity of IT projects (Parent and Reich, 2009) could be considered a good mix of factors which, together, raise contingencies which a board has to specifically look into for adequate IT governance, necessary for success.

Considering strategy-making from this study's perspective, the Contingency Theory would be helpful because adequate business-strategy formulation is contingent upon internal and external situations, including technological forces (Hofer, 1975). Since technologies have the potential of determining differences in successful organisational attributes, they pose a vital influence on strategy during increasing digitalisation. However, similar to other theories previously discussed, this theoretical perspective only views one aspect of the research area, which is the contingency brought by ever-changing technology and its impact on companies. A new model of approaching this fascinating area of research is therefore needed and proposed through this study.

The next section explores the primary theory which has the most influence and resonance with this research.

2.6.2 Guiding theory - Stewardship Theory

Having examined the theoretical influences from extant literature, one theory in specific has materialised as the most significant guide for investigation undertaken in this research. At this phase of research, the main theory influencing this study is: Stewardship theory (Donaldson, 1990). Owing to the emphasis on the stewardship perspective of a board member's role, it is understood to perhaps hold the key to the way in which cybersecurity is prioritised by the organisation. Hence, the potential to derive competitive advantage from it may likely arise from a board member's stewardship initiative, which enables the organisation to draw on that proactive stance. This theory is discussed in this section.

Donaldson, (1990) propounded through the Stewardship theory, the role played by the governing board of a company in formulating its strategies (Hung, 1998) - which included advising the executive, as well as actively participating in strategy-making (Sundaramurthy and Lewis, 2003). Stressing on the board's strategic role (discussed in 2.2.4.1.6), this theory has evolved from the insights drawn from sociology and psychology, which have influenced the belief and values of the theory. The Agency Theory (Jensen and Meckling, 1976) was then the dominant theory of corporate governance, which insisted that the governing board played a crucial monitoring role, while owning the business on behalf of the shareholders (Carver, 2000). At such a time, to imagine the governing board as stewards for the business, and not just for the owners, would have been revolutionary. To this day, the debate between these two perspectives still rages on and only in specific settings of environment, region, industry, and type, life cycle and age of the firm, does the answer emerge clearly.

Then perhaps the question lies in - where would Stewardship be applicable? The answer could be found in the psychological and sociological approaches. As Manz (1986) pointed out, stewardship motivation is dependent on stewards being able to maintain a feeling of self-determination or intrinsic motivation; we then look to the organisations which would foster a steward's intrinsic motivation. Enterprises where there exists a lack of stringent controls would facilitate trust as the basis for collective work, and promote motivation (Wasserman, 2006). Such stewards would also derive more rewards from their work (Davis et al., 1997), which would further reduce the need for control and monitoring. Findings of (Davis, Schoorman and Donaldson, 1997), which suggest that some agents pursue organisational interests even when they conflict with their self-interest, strengthens the case for when agents are inherently stewards for the organisation.

This theory has also been instrumental in furthering the cause of stewards, highlighting their behaviour and the reasons which facilitate them. Drawing further from psychological and situational factors, which promote executives to act in the interests of the organisation rather than on their own, and on whom using control mechanisms (suggested by the Agency Theory (Jensen and Meckling, 1976)) may prove counterproductive (Lee and O'Neill, 2003), we thus see that not only sometimes it is not the case of choosing the perspective of monitoring versus mentoring, it actually happens to be defined by psychological, situational and organisational factors. In the case of managing a firm's cybersecurity interests, an essential compliance to cybersecurity risk would not represent a steward's behaviour. The steward's choice, in its representation of an active strategic role, would be to proactively investigate the organisational requirement on a robust cybersecurity system, and the associated investment in it.

Drawing on Maslow's pyramid of motivation (Davis, Schoorman and Donaldson, 1997), the stewardship behaviour of executives is rooted in the self-actualisation perspective (Van Puyvelde et al., 2012), and thus departs from aligned and overlapping interests (Schillemans, 2013). This theory has also extended the study on aspects of steward-like behaviour, even asking - under which conditions does stewardship flourish (Schillemans and Bjurstrøm, 2019). It then follows that further exploration of board composition, board structure and organisational ownership are generally used as indicators of stewardship (Dulewicz and Herbert, 2004; Van den Berghe and Levrau, 2004). As we delve deeper into the aspects of strategy with regards to cybersecurity, the above characteristics of firms are bound to reflect on their choices and treatment of the subject.

Wasserman (2006) conducted a study which brought out useful insights on private technology firms. He was able to surmise that new ventures relied more on a stewardship influence, as executives who found an organisation are more psychologically involved, which leads to them acting as stewards. In the contemporary 4.0 economy, there is a clear case to explore whether such insights are still relevant and whether the conditions of fast technological advancements and higher costs of business survivability have altered the scenario. Today, all firms – even those outside the financial or technology industries – are increasingly dependent on technology. Moreover, medium to large organisations also have larger boards and executive set-ups, which could potentially further impact how the firms view their strategic role concerning IT and information systems (Hulland and Wade, 2004). This eventually will have a bearing on their approach to competitive advantage with respect to cybersecurity. Hence, in enabling a board director with the motivation to best support the organisation, this theory is best suited to explore the mechanisms involved in cybersecurity strategy, which enables an organisation to derive competitive advantage through it.

2.7 Chapter Summary

This chapter has examined existing literature within three main spheres which serve as foundation for this research, while simultaneously allowing the identification of a research gap in knowledge which this study wishes to fill. Boards and corporate governance, strategising for competitive advantage, and cybersecurity are these spheres, and they provide information of immense significance for this study.

Cybersecurity is a momentous cause of concern in the ever-changing digitalised world of today. Swift advances in the field of technology have brought with them an elevated level of uncertainty, which could be construed as both a reward and a penalty. This uncertainty can have a major impact on the competitive position of companies and, thus, warrants strategic attention (Elahi, 2013). Governing boards and their executive teams have a mammoth challenge in front of them, owing to the high stakes-high motivation emanating from the perpetrators of such cyber-threats (Chng *et al.*, 2022). The variety of breaches, novelty of new campaigns, and the dynamic nature of the cyber realm, augment the complexity involved. Additionally, no single state, organisation or official authority is capable of preventing them.

Governance of cybersecurity does not merely apply to the management of threats; rather, it extends to ensuring a framework to be in place under which all future potential threats could be readily addressed, with a top-down approach. Critical to this study is to determine how cybersecurity is integrated, or not, into the company's strategy through uncovering how the directors exercise their roles. This way the governance of cybersecurity will be positioned not only as a management of threat but also as the realisation of competitive advantage captured in the daily activities of the directors. While having strategically prepared for cyber-related eventualities, organisations still need to ensure that steps are taken, and measures adopted by all the stakeholders involved. This can only be possible when the board and top-management teams are able to chart the course of this thrilling and excitable voyage. The next chapter examines the research methodology for this study.

CHAPTER 3:
Research Methodology

3.1 Introduction

This research aims to explore the fascinating and increasingly relevant area of cybersecurity, and how boards incorporate it into their corporate strategy to derive advantages. To explore this, the chapter starts with identifying the research philosophy and the philosophical perspective which serve as the foundations of this investigation. It goes further by explaining the choice of methodological approach and research design for the study. These are followed by explaining the inquiring logic adopted, and the contextual background for this study. Next, the chapter details the level and unit of analysis and the chosen time horizon. Next, the sample, its parameters, and selection criteria are detailed. Data-collection strategy is then elucidated, followed by ethical issues and ways adopted to overcome them. The rest of the chapter details the data interpretation techniques involved in the research, coupled with details of the preliminary pilot study as well as the main study following that. It concludes with a chapter summary and a brief glance into the following chapter.

3.2. Philosophical Position

Before commencing research, identifying one's philosophical perspective is of supreme importance. Philosophy may be understood as the system of beliefs and assumptions (Saunders, Lewis, and Thornhill, 2009a), about expanding the knowledge of a specific field. All research is inherently aimed at growing the horizons of known knowledge of a given field, and a philosophical bent serves as the foundation that new knowledge is built upon. The intrinsic beliefs and assumptions of the research influence their philosophical perspective, which further leads to a decision on their research design choices.

The significance of appreciating one's respective philosophy is crucial to be able to reflect on the researcher's choice and being able to defend them over available alternative choices (Johnson and Clark, 2006). Researchers' views of the world or reality, their relationship with the subject and chosen perspective on knowledge, and their values are all essential philosophical assumptions being described here. These, thus, delineate the relationship between a researcher's view of reality and the process they use to establish it. The research paradigm for a study such as this can be understood through the following three categories of assumptions.

3.2.1 Ontological position

This assumption deals with the nature of reality, and what one may know about it (Snape and Spencer, 2003). It essentially answers the question – 'How does one view the world?' Bryman

(2008) goes further and introduces the concept of social ontology, which concerns the philosophical consideration of the nature of social entities. This perspective considers whether the social entities exist independently from social actors or are interpretations of individuals from society. This extension of the construct of ontology for the social studies realm helps identify and recognise philosophical perspectives/leanings of the social actors being investigated or explored, which supports research directly feeding back into the society.

Ontological perspective allows the researcher to decide whether the social entities being investigated are objective and factual, independent of social actors, or social constructs built from perceptions and interpretations of the said actors. Therefore, while studying a domain, it allows for a meaning of abstraction (Nasution, 2018) for creation of a new understanding of the domain, thereby helping build approaches to existing issues in it. It is also considered fundamental to the creation of a worldview and of central importance to research, thus identifying the ontological philosophy acts as the first step to any study.

Very often the nature of research – quantitative or qualitative or a mix of both - is such that it often correlates with the philosophical perspective of the researcher. For instance, qualitative research inherently views reality as perceptions and actions of the individuals of the society. Hence, it would then follow that the research philosophy would then adopt an approach wherein the researcher views the world as interpretations of the actors in it, subject to their views of them. In other cases, the research follows individuals or units whose interpretations would not influence their understanding of a phenomenon or experience. Both these cases are in contrast and would therefore reflect contrasting approaches to the study.

Two popular paradigms are often viewed as representative of differing perspectives – objectivism and constructivism (Jonassen, 1991). The former assumes that reality exists independently of beliefs and understanding, so it may be observed accurately in measurable terms. It further accepts that only the material world may be considered real, and causal links between events and what caused them may be eventually uncovered by science. Constructivism believes that reality does not exist external to the human mind and social constructs and is subjective by nature. It also assumes that social events and their meanings are in a constant state of revision and cannot be measured as they are estimates.

This study is investigating cybersecurity and its positioning within boards of directors and is thus qualitative by nature. This phenomenon cannot be measured in numbers and can only be comprehended through in-depth conversations with the governance and top management teams of corporates. How governing boards view their cybersecurity concerns; how they rate the significance of technology; how they address those, are all questions with responses being highly dependent on their subjective understanding of them. These are some examples of questions this research wishes to explore. Thus, viewing the world as subjective constructs will allow the exploration of boards, and their cybersecurity strategies which differ through various contexts, instead of a measurable terms. Hence, this research adopts the ontological position that follows from that differentiation – Constructivism.

3.2.2 Epistemological position

Epistemology relates to the view of the world as being explored by the researcher, and making sense of it (Crotty, 1998). This, in turn, is a way to respond to the question – 'How does one view knowledge?' It is the theory of what knowledge may be and the criteria used to justify it as knowledge (Petty, Thomson, and Stew, 2012). While ontology may be considered to have abstract (Saunders, Lewis, and Thornhill, 2009b) construct, the relevance of epistemology is more direct and relevant. Understanding the epistemological assumptions of the researcher is vital, as the question of what may be considered legitimate information is dependent on that perspective.

This philosophical perspective lends support to the construct of knowledge that the researcher wishes to explore, and what may be elementarily accepted as knowledge by them. Through this position, the emphasis is thus on the relationship between the actors being studied and the researcher who is conducting the study. This further leads to the identification of what is being construed as knowledge - including good data and the contribution being made to it (Saunders, Lewis, and Thornhill, 2009b).

Epistemological assumptions often follow two perspectives – positivism and interpretivism, out of other options – critical realism, postmodernism, and pragmatism (Saunders, Lewis, and Thornhill, 2009b). Within the context of positivism, knowledge is considered gathered through the collection of facts and thus is hard, tangible, and objective. Careful observations bring about value-free inquiry where the phenomena confirmed by senses can be further regarded as knowledge. Interpretivism, on the other hand, does not view independence between the researcher and the social world as a believable component since they impact each other. Knowledge is collected through the collective interpretation of the researcher as well as the participant, and is thus personal, subjective, and unique.

A study of the processes that explain how boards identify the positioning of cybersecurity within this strategy is completely dependent on how the board members view it, and how the researcher further interprets it. Whether the boards' view cybersecurity concerns as considerable or ordinary; whether the reliance on technology by certain board members is high or a moderate amount, are all examples of the distinctions of how the participants view and interpret the realm of cybersecurity strategy. The key would be the interpretation aspect of both the subjects as well as the researcher, which is bound to reflect in the way the conclusions are drawn, leading to a theory.

Together with the ontological position of constructivism, the epistemological position of interpretivism enables this research to accept the social constructs as observed by the participants, and the interdependence of interpretations of the researcher as well as the research participant, to explore the subject at hand. It follows, then, that this research presumes that the actor (board members in this case) constructs the reality, in other words, an interpretivist perspective.

3.2.3 Axiological position

This concerns the role of the researcher's values in influencing the research process, and answers the question – 'What roles do values play in research choices?' (Saunders, Lewis, and Thornhill, 2009a). The researcher's inherent views on whether their personal hopes, expectations, and values are relevant for the investigation or not influence their contribution to knowledge. Value biases may be intrinsic to the choice of the research topic, yet the way it may be contained or allowed to influence the researcher-participant interaction depends largely on their axiological position (Ponterotto, 2005).

To further determine what different *values*, have in common, values were further subdivided into intrinsic, extrinsic, and systemic values (Biedenbach and Jacobsson, 2016). Intrinsic is understood to be the actual value of something, while extrinsic is understandably a non-intrinsic or related value. Further, systemic value refers to that which follows a logical structure of something (Hartman, 1961). In the field of social sciences, the philosophical position with respect to axiology is particularly essential as it leads to the formation of future policy and/or has an impact on large groups of people like the workforce in organisations (Biedenbach and Jacobsson, 2016).

Similar to the previous two, this position also finds popularity in two possible views with differing perspectives. The axiology urges congruence between ontological and epistemological orientations (Mittman, 2001). Thus, the previously explored ontological and epistemological positions lend themselves as the inherent views on a researcher's axiological position. The objectivists-positivists are one common group of followers of this position, who would inherently believe that values, hopes, expectations and feelings have no place in the inquiry - as we have earlier understood their views to be largely reliant on facts and objective understanding bereft of value biases. In contrast, the constructivists-interpretivists maintain the interpretations and subjective nature of research, thereby being unable to eliminate the researcher's value biases in the entire research process.

The study of cybersecurity-related decision-making at the governing board's level, and its decision to pose cyber-strengths as a potential competitive choice, is primarily dependent on the views, first-hand experiences, and interpretations of the research participants – board members. Hence, this research adopts the constructivist-interpretivist approach as its choice of axiological position. The entire process of research is demonstrative of the researcher's values. By critically scrutinising the field role, to preserve objectivity as well as to reduce possibilities of contamination ((Cassell *et al.*, 2005) researcher bias), the researcher follows a reflexive approach, further lending plausibility to the findings.

Examining the above positions is elementary to this research as it helps to clarify and explicitly state the guiding foundational tone and rigour for this research. The connection between the way the researcher views the world, thinks of the world and information, and acts in the world dictate the research itself. Thus, laying the foundation to this study are the inherent positions of the researcher through ontology, epistemology, and axiology.

3.3 Research Design

Research design follows the researcher's philosophical choices as described above. To begin with, it may be useful to outline the purpose of research from among three types - exploratory, descriptive, or explanatory - as it helps provide a clear understanding of the chosen approach to research. Evident from the research question posed earlier, the research focus is to explore cybersecurity strategy and its priority within corporate governance, with a potential to create opportunities. Hence, this study is exploratory in nature (Saunders, Lewis, and Thornhill, 2009a), which is explained in detail in this section.

3.3.1 Research Approach

This research is intended for the specific context of understanding the consideration and positioning of Cybersecurity by the governing boards of companies. Through the process of data collection, analysis and interpretation of the data, the study follows an empirical method. However, such a study dealing with a limited number of participants (as opposed to a large-scale study) and investigating the experiences of the said participant group is, evidently, qualitative in nature. Since a vast majority of research can be bifurcated into qualitative and quantitative types, certain assumptions follow the respective choice.

Following a qualitative study further simplifies the possible choice of methodological approach, which could be singled out from the following typology (Creswell *et al.*, 2007; Turner, 2010):

3.3.1.1 Narrative approach

Originating primarily in literature, history and anthropology, this approach is often used to capture detailed experiences of an individual or a group. Such experiences are recorded in terms of chronological events, following a narrative, like storytelling. The focus of this approach is to gather the account of an event or actions, or a series of events or actions, which are chronologically connected (Czarniawska, 2004). As can be understood from the approach, besides the detailed experiences, their chronological sequence is of importance. Typically, the subjects being studied are one or two individuals or groups, and detailed stories are gathered to understand the possible problem.

It is most suitable when attempting to identify a problem through an exhaustive record of data collected through either interviews or document research. The methods to collect data are often not very structured, and events are often sequenced chronologically to draw sense from the comprehensive stories. In this approach, the emphasis is on attempting to outline a version of events which may be understood as a careful narrative. This interpretation of the story or events often uses a theoretical perspective.

This research draws themes and patterns from the collected data, similar to the approach of narrative methodology. However, that is where the similarity ends. This study seeks to investigate the strategy-making processes related to cybersecurity rather than create a narrative on it. Aimed at developing a generalisable theory eventually, the methodology for this qualitative study would not benefit from applying a narrative approach, which requires creating a timeline. Since a timeline does not further the cause of this study, a narrative approach is not relevant for the purpose of this research.

3.3.1.2 Phenomenological approach

This approach is adopted when the aim is to understand the essence of an experience or phenomenon. Here, the focus is often the experiences of the individuals being studied, rather than the individuals themselves. It is conducted by recording the lived experiences of several individuals who have shared an experience - through interviews, focus group discussions, observation, or document research. From this collected data, the individual experiences are used to draw out a universal essence. Here, however, the specific experiences and statements are crucial as opposed to their interpretations by the researcher, which are not being developed into a theoretical model.

The inherent idea is to reduce the experiences of the individuals experiencing the said *phenomenon* to a composite description which may be applied to a larger group. Drawing from the philosophical assumptions and perspectives of individuals' experiences leads to their description, rather than an explanation or analysis (Moustakas, 1994). Here, the data analysis, however, is very structured and detailed and often follows an inductive process. Once the essence of experience has been drawn, it is reported in plain language to be understood by the readers, which finds useful applications in the fields of psychology and education.

This research aimed at understanding the strategy-making involved for cybersecurity is aimed at developing a model to appreciate this lesser-explored realm. While employing an inductive process to capture detailed experiences of individual directors, this study is not exploring a phenomenon. Despite hopes of some degree of universality of the resulting theoretical model, it would involve interpretations of the experiences of the said governing board members and, hence, would not only be a chronicling of the essence of their experiences. Thus, an otherwise worthy approach to qualitative studies, phenomenology is not the approach adopted by this research.

3.3.1.3 Ethnographic approach

Ethnographic approach originated in the realms of anthropology and sociology. This approach is primarily used when the objective is to identify a pattern or behaviour within a particular culture or ethnography. While the data points may not be limited to a particular cultural heritage, the common group may be studied to describe their shared cultural phenomenon or behaviours and patterns within that specific culture. Here, the researcher often finds themselves embedded within the research environment and experiences of the group being studied, as they explore the experiences and environment of the group first-hand.

Data is collected either through interviews or observations, and the focus is to understand the beliefs, behaviours, and values of a particular group of individuals. The emerging themes and patterns revolve around the group roles and hierarchy or cultural identity of the group. Hence, the study tends to be particularistic (Goulding, 2005) rather than generalizable, aimed at studying a particular phenomenon or group, or their behavioural patterns. Often involving prolonged direct contact with group members, this approach is often used in the fields of marketing (to further consumer research) or medicine (to investigate a particular section of workers like emergency room employees) or social sciences.

This research, while aimed at board directors in the UK, is not aimed at exploring the cultural or behavioural patterns of such governing board members. Rather, it is seeking to explore the patterns and themes at play, while decisions related to cybersecurity are taken at the top level in companies. Instead of culture, this study investigates the several factors influencing strategic decision-making in companies, in addition to the process of such strategising. Thus, while being a useful approach in qualitative studies, ethnographic approach holds no relevance to this particular study.

3.3.1.4 Case Study approach

Case studies are used to study a problem within a case bound by either time or place. When the unit chosen is a singular case or individual, the characteristics of this approach may seem similar to that of the narrative approach. ‘Case’ may refer to an event, problem, process or activity of individuals or groups. It is used to develop a comprehensive understanding of a solitary case or similar cases with multiple perspectives. The differentiating factor from a narrative approach is that, through this approach, the primary objective is not to study the individual or unit; rather the issue about them. Moreover, as opposed to individual stories being explored, this approach seeks to investigate the entire contextual spectrum of a given case through multiple information sources.

The analytical approach involved requires a comprehensive description of the issue being studied, where the chronological chronicling of events is not essential. Here, acquiring the information from multiple data sources is key to getting a contextual understanding of the case at hand (Yin, 2003). Scholars in the past have also pointed out the importance of a *bounded* system (Kruth, 2015) – which refers to a solitary case which may be differentiated from other cases – in the context of this approach. Since multiple data sources are key, most qualitative data collection techniques like interviews, focus groups, observations, document, or artefact research, are often employed for this approach. Since it tends to explore and develop a detailed understanding of a single or multiple case/s, this approach has applications in psychology, law, political science, and medicine.

This research is aimed at forming a generalisable understanding of medium and large firms, and their strategic decision-making process related to the area of cybersecurity. Since this requires a cross-sectional study of the industry across a wide range of companies and individual directors, this study cannot gain from a case study approach. While being a rich strategy to many other qualitative studies, this research does not find relevance in the case study approach.

3.3.1.5 Qualitative Interview approach

Investigational research (Turner, 2010) has many paradigms and interview protocol is one of the most popular among them. It has a foundation in data gathered through the participants, through which the theory would eventually be developed. Detailed accounts of individual experiences are used through the process of interviews in this approach. It is most often adopted as part of the interpretative research, which presupposes interpretation to be an integral part of researcher's actions (Nielsen, 2007). Thus, an interviewee's description of their experiences in a given situation or context provides useful information to appreciate the data with respect to the subject matter.

Another element of this research is founded in the importance of interactivity in data collection - since the emergent theory would be supported by the words and actions of the research participants. The sample size is often undefined and variable and relies on being formulated into a theory appropriately drawn from the data collected through the interviews. Data collected from an inductive process is then evaluated through open codes, to draw patterns and identify emerging themes. Without reducing the role of the researcher, the information within the data, coupled with the personal values, experiences and interpretations of the researcher, lead to the forming of conclusions, in this approach.

From the perspective of this study, since the concept of cybersecurity has found significance in recent years, there is not a comprehensive body of knowledge that explains how boards position cybersecurity in their strategy. Especially coupled with investigating the processes and behaviour of boards involved in deciding how to position cybersecurity, the research topic arouses curiosity to understand this phenomenon, and help contribute towards a model/theory to explain it. The chosen sample of participating members of certain companies contributes to essential theory-building, with applications within several other company or regional settings.

Furthermore, understanding the strategic decision-making process in organisations, with respect to their technology needs, would also vary depending on a multitude of factors - like the company size, company age, characteristics of the board and industry sector. All these, and more, are expected to influence the research question this study explores. Having enumerated and briefly explained the primary methodological approaches, the qualitative interview approach emerges as the evident choice of research design for this research.

3.3.2 Inquiring Logic

Inquiring logic stems from the construct of practical reasoning (Ketokivi and Mantere, 2010), which refers to the social process by which researchers proceed from different research grounds to research claims, to establish knowledge as they understand it. To seek transparency in the justification of the claims, it is important to first understand and recognise the differing logical perspectives. Rather than be limited to philosophical positioning, it is imperative to understand the research from the perspective of reasoning - from grounds to claims (Toulmin, 2003). Furthermore, to create knowledge that may have large-scale applicability in various fields - like medicine, psychology, organisational behaviour, management, and policy – being able to distinguish between the various kinds of inquiring logic is essential.

Within the realm of social science research, inductive, deductive, abductive, and retroductive approaches are the most popular. While the inductive approach is essentially employed in generating theory from collected data, the deductive approach - in contrast - begins with a theoretical framework, which is further proved from gathered information. Abductive approach further allows for a mix of the above approaches, wherein once data is collected and a new theory generated (or an existing theory modified), it is subsequently tested through additional data collection. Retroductive approach is employed by starting with a theoretical frame, and eventually moving away from it by questioning the pre-requisites or assumptions to arrive at the framework (Meyer and Lunnay, 2013).

3.3.2.1 Deductive approach

Perhaps the most popular form of logic used in scientific studies, according to its Latin origins, deduction means ‘leading to separation, removal, or negation’ (Chiasson, 2005). Most accepted as a form of logic used to make sense of the general to a specific scenario, the deductive approach is used once a hypothesis exists or has been formed - to explicate it and test it further through various propositions. In subject areas where laws exist - which function as the basis for explanation - and are eventually controlled (Saunders, Lewis, and Thornhill, 2009b) through thorough study, deductive inference provides the best logical approach.

The deductive process of research also bears mention to the crucial work of Karl Popper and his principle of Falsification. This principle states that all claims may be proven false, in principle. In cases when no such proof may be found, the claims must likely be true (Popper, 2002). This is accepted as the central property of science being falsifiable . Considering the importance of testing hypotheses, this principle is significant to being able to evaluate them and other scientific discoveries.

Often, quantitative studies use deductive logic as it allows the study of facts, which are measured further. These facts are then drawn into multiple and nuanced hypotheses. This approach is used to match regularities previously identified, against new data (Blaikie, 2007). Testing over a considerably larger sample of units would allow for the theory to be tested, which is ordinarily the process used for deductive approach. A detailed methodology, which may be structured minutely, would be another common trait of the deductive logic. This research aimed at exploring the qualitative aspects of boards members and their strategising dynamics, is not suitable for this approach as there is no pre-existing theory to be tested.

3.3.2.2 Abductive approach

Etymological roots of the word abduction mean ‘leading away from’ (Chiasson, 2005), which influence its approach to logic in qualitative research. As a response to an anomaly or a ‘surprising fact’ being observed (Ketokivi and Mantere, 2010), it simply adopts the inference as final and sufficient to understand the conclusion. It does not require further exploration of possibilities, yet it uses additional data collection to test the underlying theory. This approach is often used for subject areas like the arts or, if adopted in the social science sphere, for the purpose of theory development and identifying findings which may have remained unanalysed (Meyer and Lunnay, 2013).

Scholars have pointed out the use of abduction in grasping the integral meaning of a subject being studied or getting an in-depth understanding of the research subject (Olsen, 2004). Furthermore, Blaikie (2007) highlights the inherently iterative nature of this process through typification and abstraction. It could perhaps be surmised, then, that such an approach is most suited to studies which are explanatory in nature rather than exploratory. For testing plausible theories, this approach could be considered a complementary one to deductive and inductive approaches (Saunders, Lewis, and Thornhill, 2009b). A study exploring a no-known existing theory or framework, seeking to understand the board dynamics at play which strategises for cybersecurity, would not benefit from this approach to logic.

3.3.2.3 Retroductive approach

Literally from its Latin derivation, retroduction refers to 'deliberately leading backward,' which implies deliberate steps of analysis and adjustment, before being framed into a hypothesis that could be further tested (Chiasson, 2005). In this approach, inductive and deductive logic are used to develop a model, a mechanism then hypothesised, and then efforts made to establish whether the mechanism works (Blaikie, 2007), thus making it an iterative process combining use of other instances. Understandably, the analysis and adjustment phases of the process would require deduction and induction, respectively. It is a process of going forward, followed by choosing to go back to understand the underlying reality of the experience. This iterative sequence, meant for a specific purpose, ensures a thorough inquiry.

Research aimed at exploring, analysing pre-existing structures, and emerging agency often relies on retroductive logic (Saunders, Lewis, and Thornhill, 2009a). This would involve a diverse range of methods and information types, depending on the subject matter which needs to be studied. It follows then, that both the popular epistemological positions – positivism and interpretivism - invariably adopt other approaches than those presented here. Thus, this research, focussed on exploring a non-historic subject matter with an interpretivist perspective, is not abiding by the retroductive inference, either. The approach used by this research is discussed next – the inductive inference.

3.3.2.4 Inductive approach

Inherently meant to convey 'leading into (or including)' according to its original Latin roots (Chiasson, 2005), this logic is the most straightforward of all approaches. Generalising from the specific case to a broad understanding for a general adaptability, this logic presents the best approach. It is particularly suited to new research areas, where existing theory is inadequate

(Eisenhardt, 1989) or non-existent, as is the situation with this study. For research areas, where the collection of data and its interpretation are meant to lead to theory development, inductive logic provides the most suitable fit. Furthermore, Blaikie (2007) explains the use of this logic to answer the *what* questions in research. The data collected offers an exploration of underlying themes and patterns, and most often leads to a conceptual framework or theory development. Hence it follows inductive reasoning, where the collected data is not aimed at verifying the theory; it instead serves as the basis for the creation of a new theoretical framework. Allowing room for explanations of phenomena that are alternative to otherwise rigid theories, this logic uses a variety of data collection methods. In most cases, the study uses small samples, in-depth investigations, qualitative methods and an interpretivistic epistemological position.

Boardrooms are as varied as can be - in terms of size, age of directors, size of organisation, CEO duality or the lack thereof, etc. Hence, making sense of their processes and dynamics involved in strategy-making, for the specific area of cybersecurity, involves numerous individual traits and features, which needs to be explored through detailed investigation. Only after a thorough data collection, can the patterns, characteristics, and common themes be identified to help develop a conceptual framework. In such a scenario, inductive logic is the only suitable one that this research may adopt. Thus, the inductive approach is used for this study.

3.3.3 Research Context

The UK first found significance in the idea of Industrial Democracy (Del *et al.*, 2013) and soon thereafter, graduated to a concept of wider importance of Corporate Governance in the early 1990s. Beginning in 1992 and successively, the Cadbury Committee, Greenbury committee, Hempel committee and later Higgs Committee, have all contributed towards setting of regulations for the field of corporate governance in the UK (Del *et al.*, 2013). Cumulatively they have highlighted the responsibilities of executive directors, the independence of the non-executive directors, the emphasis on tightening internal financial controls, and the procedures for reporting. In contemporary times, the world of corporate governance is also evolving.

In this knowledge era (Uhl-Bien, Marion and McKelvey, 2007), relevant new concepts ranging from *Internet-of-things* (Radanliev *et al.*, 2019), *Artificial Intelligence* (Möslein, 2018) to *blockchain* (Yermack, 2017), have shifted the paradigm. Thus, the boards which incorporate these technological changes/trillion-dollar opportunities into specific new business models, strategies and practices are the new success stories (Grove and Clouse, 2017). Recent literature highlights the characteristic features of contemporary technologies of the 4.0 economy enumerated above – automation, intelligence, and connectivity (Piccarozzi, Aquilani and Gatti, 2018). These information and communication technologies have surpassed the advancements of before, thus creating endless unprecedented opportunities for businesses.

As underscored by the research context, the challenges presented to the governing boards of organisations in the knowledge era, to strategise a competent policy for cybersecurity is complicated. Unlike the world of even a decade ago, when advancements in technology were relatively less impactful, the contemporary organisational domain is markedly altered. Thus, while boards and management have always strived to craft a strategic policy plan that would allow the firm competitive benefits against its rivals, the same task in an interconnected cyber realm without borders is magnified. How, then, do governing boards with assistance of their executives, work their magic? This and other curiosities related to the role of strategic decision-making in the context of cybersecurity thus allow the UK as an excellent area to explore this subject.

In a broader context, this research explores the fascinating world of cybersecurity strategy in organisations from a wide variety of industry sectors. This is on account of the varied degrees of impact faced by different industries. While the financial and/or critical infrastructure may be considered more vulnerable owing to the nature of information and data stored in their cyber assets, the public sector attracts considerable interest from threat actors on account of its lower risk status. It is understood that the degree of motivation to adopt a more cyber-aware stance may also vary within each industry sector; it also necessitates a wider scope of such sectors (including private and public sector organisations) to investigate a more holistic and authentic response to the research question, which is not skewed in the favour of a minority of industries. A detailed description is followed in Sample Selection 3.3.7

3.3.4 Levels of Analysis

The level of analysis for this research is presented by the individuals concerned with crafting and implementing the cybersecurity strategy for the organisation. Thus, the level of analysis (Yurdusev, 1993) is that of the governing board members and executives based in the UK, even though they may represent organisations which are based in different geographies.

3.3.5 Unit of Analysis

This study is keen to explore the way the board directors, in tandem with their executives, craft and implement their cybersecurity strategy - with the potential to derive competitive advantage from it. In this case, it is vital to find the perspective of these individuals who are involved in these processes, namely - the governing board members, and the members of the executive committee associated with cybersecurity. These individuals thus present the unit of analysis for this study.

3.3.6 Time Horizon

This study has been conducted in a cross-sectional study, capturing a moment in time. This is specific considering the impact of digitalisation and, even more particularly, the impact of the Covid-19 pandemic on organisational routines associated with accessing cyber domains and their overall defence mechanisms. As the future directions of the research section in 5.8 would expand on, a longitudinal perspective would certainly expand on the work of this study. However, that perspective has not been adopted by this research, at this time.

3.3.7 Sample Selection

Having identified the appropriate inquiring logic, the next step is to decide the parameters of the sample. This involves determining details of how data is to be collected and from whom. Since data gathering is crucial towards better understanding of the given theoretical framework in place, the manner of collecting data and choosing informants with sound judgement are imperative (Bernard et al., 1986). Thus, to arrive at the most effective theoretical framework within its respective field, this study adopts the research strategy most conducive to collecting the desired data/information consistent with its research question.

3.3.7.1 Sample specifics

This research explores strategy-making in organisations, which allows governing boards to position cybersecurity as a potential competitive advantage. Strategy related decisions are taken at the top of the corporate pyramid – by the board of directors, in association with other members of the C-suite (chief executive suite). It would thus follow that this investigation bears fruit when conducted with such authorities of the arena. Purposive sampling method allows data gathering from a set of knowledgeable experts from a particular field, in a non-random manner of selection.

Elite interviews address the questions related to positioning of cybersecurity within corporates. As discussed in the literature review earlier, literature supports the view that strategy-making is conducted in organisations at the top (the governance level). Thus, to investigate the dynamics involved in cybersecurity decision-making from a strategic perspective, these interviews are organised with the governance team in organisations, which comprises primarily of their board members - including both executive and non-executive directors - in addition to the vital members of the executive committee involved in cybersecurity associated decision-making.

Further, the companies under study are from a wide array of sectors ranging from financial services to education. Financial services as an industry has had extensive experience with online management of information, as well as access to extremely private customer data (including financial information). Hence, they have had to pre-empt cyber threats and safeguard user information more securely than their industry counterparts. The transport sector has recently shown increasing impetus in their online realm. It is thus reasonable to imagine that this dependence on the cyber world is expected to rise. Hence, financial services and retail industries serve as the two ends of a relevant spectrum for this study. The entire sample is a range of organisations, instead of following one or two sectors to gather the data, thus allowing for heterogeneous sampling - to understand key representative themes.

With increasing concern for the size of sample sensed for social research (Hammersley, 2015) in recent years, many academics have pointed out the difficulty in predicting an exact figure that might be required in studies of qualitative nature. However, Blaikie (2018) reassures that indicating a range of sample size may be acceptable, consistent with the subjective nature of qualitative social research. Determining the sample size for this research would be from two parameters:

- on availability of access to the required informants
- on the collected information reaching data saturation

On the basis of existing literature, it is understood that an effective number of informants for a qualitative interview sample could be 25-30 individuals (Creswell, 2007). These individuals, representative of their respective corporate culture, processes, and organisational behaviour would reflect the key illustrative themes. This research first interviews a set of 10 informants and gathers in-depth information. After garnering useful feedback, and reflecting on the information gathered, interviews are conducted with 20-25 more informants to extend the sample with the subsequent cases. It may be considered a reasonable expectation to imagine that the above sample should allow saturation of both description and explanation (Blaikie, 2018), on which to further base the development of a framework.

These are in-depth interviews (audio recording wherever permitted by the individual interviewee) with different members of the strategy-making team in different companies, lasting between 30-120 minutes each, requiring adequate preparation. The admittance to such a restricted circle of informants, and the process of detailed information-collection, realistically requires over six months. Access to such elite personnel is initially sought through the privileged network and professional associates of the 'gatekeepers' (Devers and Frankel, 2000) overseeing this study – research supervisors. In addition, the benefit from extended acquaintance with the initial interviewees is also sought as a way to expand the desired sample.

3.3.7.2 Methods of sampling

There are different methods of sampling available for qualitative research. Probability sampling is primarily used to test hypotheses empirically; hence the elements are chosen at random with a known probability of being sampled (Lewi and Ritchie, 2003). This method finds popularity with quantitative research. On the contrary, in qualitative research, the essential concern is not to be representative of the larger population or even testing hypotheses, so the primary method employed is non-probability sampling. This sampling focuses on deliberately selected samples to reflect particular features of or units from the population.

Non-probability sampling is also followed through a few different methods. Key among them are the following types:

3.3.7.2.1 Convenience sampling

This type of sampling is also known as availability sampling and is employed in cases which lack a clear sampling strategy. Here, the researcher selects their sample on the basis of ease of access and availability. It is often considered one of the most popular forms of sampling, using data from people or other relevant sources with the most convenient access. While these participants may often be volunteers, this technique does not preclude theoretical representativeness (Johnson and Waterfield, 2004).

In this type of sampling, deciding the right size of data collection may be a crucial decision to make, as too much may lead to a superficial analysis, while too little may lead to the loss of important perspectives and themes (Sim and Wright, 2000; Malterud, 2001). Also, this type of sampling is prone to bias and influence beyond the researcher's control as the data is collected only on the basis of ease of collection (Saunders, Lewis, and Thornhill, 2009a). Used often on student projects or exploratory research, this may not be the most appropriate method to draw conclusions about larger populations.

3.3.7.2.2 Snowball sampling

This method is employed when existing sources of data are used to identify other people, they may be connected with who fit the criteria for selection. Particularly useful for small or dispersed populations, this method is considered best suited as a supplementary technique for sampling. This method could be considered useful in cases where there is apparent difficulty in either identifying cases (Saunders, Lewis, and Thornhill, 2009a) or gaining access to them.

Owing to the slow nature in collecting data through snowball sampling, the number of cases may be low; however, they are expected to have the desired characteristics expected from an ideal sample. Relying wholly on this method may lead to a sample frame where the diversity of the sample may be compromised (Lewi and Ritchie, 2003), as the new members of the sample are generated from existing ones.

3.3.7.2.3 Quota sampling

This technique of sampling is another method of non-random sampling wherein the sample is considered representative of the larger population. This is because the variability of the quota variables in the sample is the same as that in the population (Saunders, Lewis, and Thornhill, 2009b). In this technique, both representativeness - of the actual population and control over the sample - are high. Quota sampling is often employed with interview surveys such as market research or political opinion polls.

This is an alternative to the probability sampling techniques, where data is needed to be acquired over a relatively brief period of time. Understandably, this sampling is mostly used on large populations, where the sample size could be between 2000-5000 (Saunders, Lewis, and Thornhill, 2009a). Used for stratifying the data, quota sampling is helpful when the researcher may be able to overcome possible variations between diverse groups of the population. Here, the focus is selection of the most appropriate sample - in terms of size and weightage - in a way to have sufficient responses to be able to derive actionable results.

3.3.7.2.4 Purposive sampling

Purposive sampling is a means of sampling where the participants are chosen deliberately owing to the characteristics which make them suitable for selection. This is a form of non-probability sampling procedure. This method is also known as judgement sampling, as the sources of data are judged to be eligible for being sampled for research. It is often employed in cases where the focus is either on key themes, or importance of a case, or even in-depth understanding (Saunders, Lewis, and Thornhill, 2009a). Godambe, 1982, highlights the importance of knowledge and skill of the informants, so as not to render the data meaningless and invalid; thus, the above selection makes for the most appropriate selection.

This method is often adopted when collecting information about knowledge of a given field not known to all the members. Depending on the nature of the research question and the objectives of the research, this sampling technique may be considered most effective. For the purpose of this research, the types of participants mentioned earlier are the individuals with the desired access, inclination, and resources to support this nature of investigation. Appreciating the cybersecurity-related strategy choices of an organisation through their governing board dynamics is a specific purpose that justifies the choice of this sampling method.

Hence, purposive sampling (Tongco, 2007) is the main basis of selecting samples for this research. In addition, whenever possible, the researcher supplements the sample through the snowballing technique (Goldstein, 2002) as well. A judicious combination of both techniques enables a rich sample for this study.

3.3.8 Data Collection Strategy

The next step is to elucidate the required data-collection method suitable for this study. Looking at the background, the first methodological wave in the fields of behavioural and social sciences was dominated by quantitative paradigms, as early as the 19th century (Onwuegbuzie, Leech and Collins, 2010). However, from the 1950s, qualitative paradigms came into the spotlight and have evolved from a logical perspective of quantitative methods to a reliable and objective viewpoint of qualitative ones. This research, being in line with qualitative paradigms, would follow such a method of data collection.

Qualitative methods are considered robust for their ability to capture data with more depth and detail, as the primary instrument used to collect and interpret data is the researcher themselves (Ochieng, 2009). However, different persons would interpret the same situations differently and, therefore, any or all methods conducting qualitative research require that the emergent range of possibilities may be observed. Miles and Huberman, 1994 discuss two possible biases (until addressed) - the first is when the researcher affects the participant; the second is when the participant affects the researcher. This research thus takes advantage of the above-discussed (section 4) reflexive approach and technology-led organisation and examination.

Having addressed the challenges of data thus collected qualitatively, there exists an array of methods to choose from, which can broadly be categorised into four types (Onwuegbuzie, Leech and Collins, 2010):

3.3.8.1 Document/material culture

This refers to the written text or cultural artefacts which are otherwise beyond the scope of interview or focus group and yet hold the key to the underlying lived experiences of the person or group under study. The documents or material culture present evidence of gendered, social, cultural, and political construction - which give a descriptive idea of the individual or group being researched. This could include the white papers, documents, memos, and company minutes recorded for official meetings. Interestingly, since this method is not derived from spoken words or discussions, it is available over a period of time and provides a historical insight (Onwuegbuzie, Leech and Collins, 2010).

In contemporary times, to preserve such documents for posterity as well as to gain access to it sometimes, technology offers major support through various software and hardware means. Over time, this collated evidence can even show the growth or progress of the researcher. Often, this method is used as a supplementary means of collecting data either prior to (or after) other forms of data collection have been employed. At other times, when access to sources of information is otherwise limited or alternatively virtually available, then documents or material culture provide ample resources.

From the perspective of this study, documents singularly do not provide adequate information to base the development of a new theoretical model on. Understanding the board of directors' processes and motivations while framing their cybersecurity strategy cannot be comprehensively studied through the vast volumes of data available, both offline and online. Company information through reports, meeting agendas and press coverage provide preliminary information to create a foundation for other methods of data collection to then build over. Hence, the search for the most appropriate method for data collection for this research still continues.

3.3.8.2 Focus group

Focus group discussion is a form of non-standardised interviews conducted in group, although they differ from group interviews. This research is used to collect data from more than one individual at a given time, regarding a specific area of investigation. This method is used when the topic is pre-defined, and the focus is to enable interactivity between the participants. (Saunders, Lewis, and Thornhill, 2009a). Since this method uses simultaneous investigation from multiple sources, it is often considered economical as the data can be collected faster and at a lower economic cost to the researcher.

Another elementary feature of such a group is that it presents a collective view and is not individualistic in nature. However, a combined interaction such as this may even encourage participants to feel safe and less inhibited and may lead to more responses from them. This is particularly useful when the participants are shy or otherwise reticent, and a group setting may help bring up topics or conversations, which puts them at ease. This method is also used in cases where the participants are from similar backgrounds and the experiences presented are not expected to be divergent. A homogenous nature of participants, needed to be explored in an in-depth manner, may be conducted through focus group discussions.

However, in cases when individual experiences being captured in truth and range is essential, having a group setting may not be extremely useful as it does not allow much flexibility within the group. Also, in certain cases, the group dynamics may interfere with complete or accurate data (Walker, Ives and Damery, 2017) and, hence, focus group may not be the method of choice. In the case of this research, the data to be gathered rests largely on the individual experiences of the board members - which are expected to be diverse and varied. Also, the data to be collected is from an elite stratum from the companies – their board directors – and it may not be feasible to have many of them simultaneously available for an open interaction. Hence, focus group discussion, while a veritable method of data collection, may not be the most practical choice for this study.

3.3.8.3 Observations

Observation in qualitative methods is one of the oldest forms of data collection, conducted through observing. It has been considered the fundamental base of all research methods (in social and behavioural sciences), according to Adler and Adler (1994). The basic process is to observe, create a checklist and observe again (Walker, Ives and Damery, 2017). Literature traces multiple ways to record observations though, primarily, observations refer to the stylised notes taken after an event or series of events have taken place by one or more observers.

There could also be use of photographs, visuals, or videos to record the insights gained. In certain settings, a wearable camera system (self-cam), which allows collection of video and audio movements, may also be used to collect observations (Teeters, 2007). These notes or visuals are often collected over a period of time, often coupled with another activity as a complementary method to capture data. This method is also used when the researchers are more than one, and since the observations are made by all, they increase the possibility of reliable results (Walker, Ives and Damery, 2017).

However, these are often reliant on the interpretation, insight, perspective and recording mechanism of the person recording the data. This may lead to the accuracy of the data being somewhat constrained and may not compete successfully with other more reliable forms of data collection. For the purpose of this research, observations alone would not serve the entire purpose and requirement of data collection. Understanding the prevalent themes during strategy-making for cybersecurity requires more of an interaction with the key players in the decision-making, namely the board directors. Observing them and learning additional cues - from interactions with them - could be certainly useful but it would need to be supplemented with another form of data collection.

3.3.8.4 Interview

Essentially, an interview is a purposeful discussion between two or more people, in the words of Kahn and Cannell (1957). Unlike questionnaires, they involve a relatively free-flowing interaction between the participant(s) and the researcher (Saunders, Lewis, and Thornhill, 2009b). Categorised as structured, semi-structured or unstructured, interviews are methods to collect one-on-one information. Compared to quantitative research, these offer greater ecological validity, providing insight and ability to draw understanding of the complex organisational realities (Eby, Hurst and Butts, 2009).

Structured interviews are pre-decided and planned in terms of the various details involved, such as the length or duration of the interview and questions to be raised. Unstructured interviews on the other hand, are left to follow the flow of the interaction between the participant and the researcher. Any detail may not be expected to be known in advance in such interactions. Semi-structured interviews are in-depth and may vary in length, theme, variety of questions asked, and the level of formality. Both verbal and non-verbal forms of communication are exchanged during interviews, which provide additional and supporting information for the researcher.

Since this study intends to explore a range of issues faced by the board and management of companies in today’s cyber-enabled world, the most appropriate method to collect information is through semi-structured in-depth interviews. Within companies, only the governance team and top management have access to such data. Hence, elite interviews would be with non-executive directors, executive directors, risk officers and members of committees dealing with risk and compliance, within mid-level to large companies in the UK. This research is functioning on the assumption that small companies may not have the necessary resources or experience to have dealt with the strategic reasoning to approach cybersecurity from a necessity perspective.

Cybersecurity is a topic that needs to be strategised at the top of the company pyramid, instead of just its IT department. Some companies hire non-executive directors with prior experience in the field, while some others hire specific executives trained for the field; yet others designate committees and members to address the issues of risk through cybersecurity threats in companies. If cybersecurity were to be treated as more than just an exigency - especially as a strength - it would need the vision and acceptance of the board. Hence, detailed conversations through the above-mentioned elites (Nicholson and Cameron, 2010; Harvey, 2011) are expected to throw light on and answer the research question posed earlier.

Additionally, through notes and observations of the interviewees, the study aims to cross-reference the data to aid corroboration. It is understood that observational data could serve as a significant source of understanding this fascinating subject. Finally, collation and consequent analysis of this collected data reveals the true attention necessitated by cybersecurity.

3.3.9 Data Analysis Strategy

Any collected data is inconsequential until it can be organised and managed through coding, themes, and patterns. However, choosing the appropriate analysis method is crucial for leading towards such learnings. Such approaches inherently allow certain data analysis methods, of which language-based methods may be classified in the following popular types:

3.3.9.1 Content analysis

This practice is used to analyse language, to describe content by examining who says what, to whom, and with what effect (Bloor and Wood, 2006). Especially for phenomena where there exists inadequate knowledge, content analysis may be used to highlight common problems mentioned in the data. Content analysis is useful in its ability to simplify the content by understanding the in-depth meaning conveyed in it. To ensure robust understanding from this data, it is of key essence to collect data from multiple sources - whether they may be text, audio, or visuals (including images and videos).

This form of analysis is used for recording the numerical frequency of codes (Bennett, Barrett and Helmich, 2019), patterns, concepts, and themes in data in a non-invasive manner. While it shares some common features with Thematic Analysis, it is unique in that it allows data analysis qualitatively while recording the said data quantitatively. However, for highly open-ended holistic research unable to be labelled in categories, this popular method may not be appropriate (Mayring, 2000). Thus, it finds fields like marketing, media, and literature as the most popular realms for its usage.

Useful for enabling extraction of the essence from a large amount of data, this form of analysis is often employed to describe the characteristics of the content. In many cases, from a large volume of data, content analysis supports the argument that can be drawn from it. From the perspective of this research, while analysing the content is helpful, there are more expectations from the analysis method. The analysis is required to be able to draw themes and patterns from it, which would further enable the development of a theoretical model. Without any necessity to support an argument, this study - aimed at understanding the governing boards which strategise for cybersecurity- needs a data analysis method capable of extracting themes otherwise not prominent or well-formed.

3.3.9.2 Document analysis

Documents in the form of notes, case reports, contracts, drafts, annual reports, and other official documents are used for the purpose of this analysis (Flick U, E von Kardorff et al, 2004). Official documents may be intended for specific recipients while simultaneously being the designated means of drawing legitimate conclusions. This method employs a systematic method of analysing documentary evidence for drawing meaning and empirical construct from them. Carried out iteratively, document analysis requires thorough examination and review of the documents being studied.

This method also involves the coding of content into themes, like in some other methods. However, unlike those methods, it allows for the potential independence of meaning conveyed within the document since it does not employ reduction and paraphrasing of text. Rubrics are often used to review and interpret the documents being analysed. It is primarily used to understand structural issues and implications of presentation choices in both the public records and personal documents being studied.

Often, this method of data analysis is employed in mixed methods study to triangulate and corroborate findings from other data sources. For the purpose of this study, whose objective is to draw an understanding from the behaviours and processes of the boards of directors of companies, as they make decisions regarding cybersecurity policies, document analysis may be inadequate. It may offer useful understanding of some of the documents being used to study governing boards, but to be able to draw themes from the above research would require more sturdy and reliable methods to analyse the data.

3.3.9.3 Discourse analysis

Discourse analysis is used to explore the meaning produced in language use and communication, and the contexts and processes of these meanings. This practice analyses the use of language at a micro level and the situations it is used in, at a macro one (Tannen, Hamilton, Schiffrin, 2015). Often used for studying organisational contexts, this mode of analysis is useful for studying key theoretical positions. Empirical material, which is typically linguistic in character, may leave much to be interpreted and drawn from text and its function. This deficiency is worked on through discourse analysis.

Essentially, it is used to understand the impact of language through speech or text on construction or changes in the social world (Phillips and Hardy, 2002). When it is used to analyse data from the point of view of power and empowerment, it is further classified as critical discourse analysis. Understood from different perspectives, this form of analysis provides an essential bridge between language and its relationship with the people using it. Discourse analysis provides the basis for appreciating the characteristics of the people instead of the text itself.

While there are no generally accepted fixed methods of conducting this analysis, there are certain key strategies adopted for its use. Useful for studying language and its applications in various texts and contexts, discourse analysis is not the most suited for this study. While language is used to describe processes and behaviours of board members, and their first-person accounts forms the basis of content available to be studied, the study moves beyond the immediate scope of the language. Instead, the prevalent themes and emerging patterns need to be studied and analysed through other means to enable theoretical contexts to be conceptualised from them.

3.3.9.4 Narrative analysis

This form of analysis is employed to explore the linkages and relationships underlying (Saunders, Lewis, and Thornhill, 2009a) narrative accounts, such as autobiographies. This method aims to identify the kinds of stories told as well as the stories used to represent the researched phenomenon in culture and society. The final product through this method creates generalisations of attitudes, actions, and meanings associated with the phenomenon.

The phenomenon being studied is further categorised into concepts, terms, and points of view, but not in themes like other methods. Interestingly, there is much debate within the academic community regarding whether the result of the analysis must also adhere to the confines of a narrative or story. In that context, the narratives then are not just recounted by the contributors and sources, they are also created by the investigators researching the phenomenon or stories.

Understanding various aspects of the story presented – including the story's structure, function, and essence – are the primary elements being analysed through method. As this type of analysis essentially relies on data in a storied form, it may not be the most suited for this study. This research, through primary data collection methods like in-depth interviews, seeks to understand the board's strategy-making for cybersecurity decisions. While the format may inherently exist in a question-answer and experience-relating context, the narrative element may not be consistently present. Furthermore, neither creating a narrative nor following a narrative structure is required for this research; hence another data analysis method is employed.

3.3.9.5 Thematic analysis

As may be understood by its name, this method of data analysis is employed to identify, analyse, and report patterns/themes within data (Braun and Clarke, 2008). While it is similar to other approaches in its practice of identifying patterns, it is dissimilar in its lack of association with a pre-existing theoretical framework. Thus, it allows the flexibility of being employed in either an inductive or deductive approach (which each study outlines prior to collecting data). It is particularly useful for studies where the themes are abstract and often identified by the researcher during the process of study (Ryan and Bernard, 2000). Whether the data being studied is text, audio or video, this method of analysis is the most popular to help simplify the data being studied and identify common themes from it.

Initially used in the field of psychology, this form of analysis quickly evolved to be used in the field of sociology to effectively draw out simple themes from complex data. It is useful for being able to draw research findings which are insightful, rich, and trustworthy (Nowell *et al.*, 2017). Essentially using three steps (Bennett, Barrett and Helmich, 2019) – descriptive coding, interpretive coding and identifying overarching themes – this method is used with a wide variety of methodologies. As King (2004) points out, thematic analysis is useful in studies comprising large data sets which guide the researcher through a structured approach to handling the data in creating an organised final report.

Considering the specifics of the research question, philosophy, methodological approach, and strategy of this study, one approach emerges as the obvious analytical tool of choice – Thematic Analysis. Cybersecurity positioning as a strategic decision of boards is an exploratory topic, which relies on exhaustive data collection from board members to help identify and draw out themes. Working with constructivist leanings and an inductive approach towards theory development, requires an analysis method that allows flexibility of subjectivity. Furthermore, this study requires the researcher to be an active component of the process, which is another trait of thematic analysis approach.

3.3.10 Researcher Involvement

Not limiting the question of validity to the wise judgement and keen insight of the reader, as pointed out by Sandelowski and Barroso (2002), there would be other ways to ensure it. (Whittemore, Chase and Mandle, 2001) highlight the primary guiding features of validity as credibility, authenticity, criticality, and integrity; explicitness, vividness, creativity, thoroughness, congruence, and sensitivity are the secondary criteria. This study - through its industriously sought-out sample to be studied, painstaking data collection and comprehensive data interpretation strategies - aims to highlight the above features of integrity, authenticity, and credibility as a means to justify its validity.

While subjectivity is a cornerstone of qualitative study, and this study views it as a key strength, it is often predisposed to judgements on account of validity. Consistency is one pillar in the overall work; between the described method and reported analysis, language and philosophical position, and themes drawn out. Trustworthiness as delineated by Lincoln and Guba (1985), peer debriefing, and reflexive writing throughout the entire study, is another strategy to ensure this study's validity. Marshall (1990) confirms honesty and forthright investigations to be the defining features of quality research, and this study endeavours to ensure the above characteristics are portrayed unequivocally.

3.3.11 Ethical Considerations

Tracy (2010) among other scholars has identified eight 'Big-Tent' criteria for excellent qualitative research, among which *ethics* holds a significant position. Other voices in academia have reinforced the importance of clear, ethical consideration and conduct (Whittemore, Chase and Mandle, 2001), especially in a qualitative study. Since the information collected is exposed to misinterpretation, exposure, exploitation or not even being factually shared for fear of any possible misuse, outlining the probable ethical issues and ways to overcome is almost sacrosanct. In cases of qualitative research, when the participant is sharing personal or often classified information through words, behaviour and body language, the responsibility to ensure its ethical use could be considered higher than for quantitative studies.

The University Research Ethics Committee allows schools to operate their own ethical procedures within strict guidelines laid down by committees. The researcher sought the University of Reading's approval regarding ethical considerations, data confidentiality and data protection prior to commencing the research. Thus, in keeping with the above-mentioned guidelines, the researcher has outlined the following ways to ensure that the informational integrity is maintained. The entire data collection process is segregated into the recording of information first, followed by maintaining its confidentiality.

3.3.11.1 Recording of data

The original and intended model of data collection was meant to be physical one-to-one interviews with the governing board directors or top management team members of the given sample set. However, the Covid-19 pandemic, and its globally limiting impact, rendered the physical interviews infeasible. The next best alternative adapted under the external scenario, was to conduct virtual video interviews online through popular video calling software such as Skype or Microsoft Teams. Since the University of Reading has affiliation with Microsoft and all researchers are members of and have access to secure MS Teams software, it was finalised as the implement to conduct virtual interviews.

These interviews were recorded on Microsoft Stream (with consent from the participant) so as to enable ease of transcribing the conversations, in addition to being able to refer back to the dialogue for multiple use. These recordings supplement the notes taken from the interviews, to add to the robustness of the data collected. Additionally, the recordings also help avoid any bias of the researcher’s version of the interview, with actual recording and transcript from the interview guiding the study. Moreover, to avoid any misinterpretation of the data and/or any misunderstanding of the information, the recorded version adds an additional layer of reliability.

The physical interviews were audio-recorded so as to help with transcription (with requisite consent of the participant), with some of them also including videotaping (whenever possible; again, with the participant's consent). These were conducted at the workplace of the interviewee during working hours, so as to facilitate credibility of the information collected. The difference between a place of comfort and confidentiality (like the personal office chamber and a coffee shop) is stark, and the researcher took steps to ensure that the participant was at an ease sharing such qualitative and confidential information.

Finally, being a part of qualitative exploration, actual body language, tone and voice modulation of the participants’ responses guided the actual information collected from these sessions. Thus, recording the interviews was especially useful to rely on while conducting data analysis in the next stage.

3.3.11.2 Maintaining data confidentiality

Once the information is collected, it is of paramount importance to devise processes and protocols to ensure that the content remains confidential and is not exposed to abuse. First and foremost, all personal identifiable information of the participants and their organisations was replaced with the researcher’s identification codes, which allowed ease of identification while simultaneously keeping the owner’s identity concealed. Furthermore, the identifying features of the participants were not limited to their names alone; instead, through a combination (of other variable identifiers specific to them) being used in the collective form, or as excerpts from non-identifiable individual sets.

The access to the data itself was protected through a key of the master code list, which was limited to the researcher only, to avoid exposure to any unrelated parties. Moreover, the files containing any electronic data related to the participants were password protected. At times, when computers were not in use, the folders were closed on the computer, limiting access and visibility. With cybersecurity concerns being real and considerable, whenever the participant information was exchanged or shared over the internet, the files were encrypted for protection.

Finally, with virtual cloud storage being another crucial tenet to cybersecurity, even the above information was stored exclusively on the University of Reading's One Drive and will be destroyed post use – three years from date of completion of collection. The above processes are some of the measures taken to ensure that the integrity of the data collected is ensured and that it is not exposed to any vulnerability – virtual or physical. Rigorous following of the above processes enables the rendered data to be ethically sourced and maintained, and aids in keeping its integrity intact.

3.3.12 Summary of Research Design

This section concludes a description of the chosen research design for this study. The philosophical foundations chosen were constructivist and interpretivist perspectives, for ontological and epistemological positions, respectively. Qualitative interviews were chosen for the research approach, while inductive logic was followed for the choice of inquiry. Research context explains the choice of individual board members in a wide range of industry sectors within the UK, within a cross-sectional time horizon. The sampling strategies involved a mix of purposive and snowball sampling. The data collection was conducted through in-depth elite interviews, while the analysis was conducted through thematic analysis. This section concludes with an explanation of the methods adopted to uphold high ethical standards.

*Table 3.1 Summary of Research Design. **Source**: Compiled by the author.*

Elements of Research Design	**Details of Element**	**Design Choice**
Philosophical Position	Ontology	Constructivist
	Epistemology	Interpretivist
	Axiology	Constructivist-Interpretivist
Research Design	Research Approach	Qualitative Interview
	Inquiry Logic	Inductive
Research Context	Broader Context	Organisations across multiple industry sectors
	Level of Analysis	Board members
	Unit of Analysis	Individual
	Time Horizon	Cross-sectional
	Sample	Purposive and snowball

Data Collection Strategy	Data Collection Method/Technique	Interviews (Elite)
Data Analysis Strategy	Data Analysis Method/Technique	Thematic Analysis
Ethical Considerations	Recording of Data	Microsoft Stream
	Maintaining Data Confidentiality	Restricted to researcher access

3.4 Pilot Study

The pilot study was instrumental as an initial step into the more comprehensive data collection planned for study. Identifying appropriate participants, accessing them, and engaging with them in fruitful discussions about cybersecurity strategy was aimed at these corporate elites through in-depth interviews (Goldstein, 2002; Harvey, 2011; Mikecz, 2012) based in the UK. The following section describes in detail the methodological components of this pilot study.

3.4.1 Purpose of the Pilot Study

The purpose of the pilot study was to ensure the appropriateness of research methods and viability of the research question (Miles and Huberman, 1994). It was thus conducted to acquire an informative glance on the field, appropriate ways to approach the research, adequate methods to carry it out and refine the means as required. Also, it was extremely useful in gaining an improved perspective on the main data collection for this study.

3.4.2 Pilot Study Sample

The research necessitated that the elite interviews be conducted with the directors of governing boards of organisations, who were residents of the UK. The pilot study primarily focussed on board members from companies from the technology industry or those who functioned as technology consultants to other industries. These participants were in positions which allowed them first-hand experience of cybersecurity strategy-making in their respective organisations.

3.4.3 Pilot Study Data Collection

Accessing the participants was conducted through the extended professional network of the researcher. These interviews were conducted with three different board members, who shared their views and experiences associated with cybersecurity decisions in governing boards. Interviewing these participants through hour-long in-depth conversations assisted in gaining insight into the perspectives of governing boards strategising for cybersecurity.

The elite nature of the interviews necessitated the researcher to conduct adequate prior preparation (Chase, 2005) with respect to background information about the participants before conducting the interviews. This was conducted through the available news articles, publicly available previous interviews, profile information from company websites, professional networks like LinkedIn, and even their blogs or articles posted online. Owing to the extensive impact of Covid-19 and its subsequent effects, data for the pilot study was collected through in-depth one-on-one interviews on Microsoft Teams (Archibald *et al.*, 2019; Jones and Abdelfattah, 2020; McKinley *et al.*, 2020). These were recorded for future observations and transcription with approval from the participants.

3.4.4 Pilot Study Data Analysis

Systematic qualitative procedures of coding, according to Strauss and Corbin (1990), emphasise the steps which began with *open coding*, wherein the researcher drew the primary categories from the textual data. This was followed by *axial coding* which required the researcher to build a model from the open-coding categories. Finally, *selective coding* was used to take the model and draw propositions from it (Creswell *et al.*, 2007).

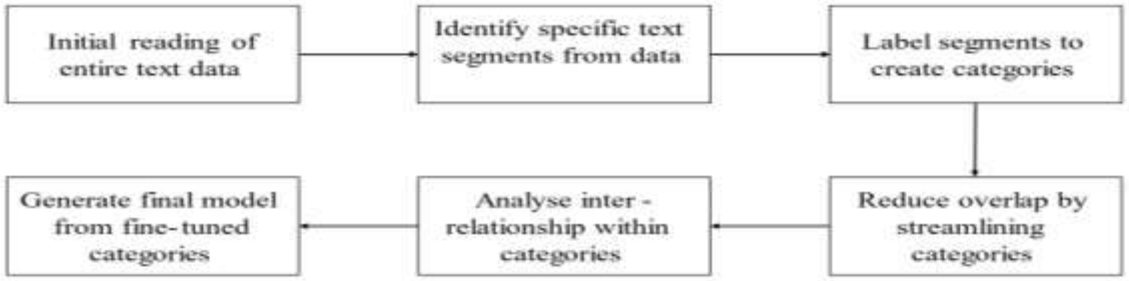
Initial reading of entire text data
Identify specific text segments from data
Label segments to create categories
Reduce overlap by streamlining categories
Analyse inter - relationship within categories
Generate final model from fine- tuned categories

*Figure 3.2 Coding process. **Source**: Adapted from Thomas (2006)*

The process outlined in Figure 3.1, enumerates the process flow of the steps taken by the researcher to draw emergent themes from the textual transcription of the data.

3.4.5. Pilot Study Findings

Inductive coding was conducted on the transcribed data from the in-depth interviews. After repeatedly reading the textual data, certain codes and labels emerged, which were then assigned to identify the categories and interpret the data (Thomas, 2006). Meaningful sections were effectively marked as categories, which further helped unearthing the dominant themes and patterns.

Terms used to identify the categories were those used by the researcher during the elite interviews (Strauss and Corbin, 1998) and others inspired by the literature reviewed earlier. Broad categories like board roles, board behaviour and dynamics, technology significance and decisions, cybersecurity factors, cybersecurity decisions, and pandemic were key in the interview data. These further enabled an understanding of the labels available within these categories.

Following are the themes which emerged from the analysis of the pilot interviews:

- Board roles
- Board Behaviour and Dynamics
- Technology Significance and Decisions
- Cybersecurity Factors
- Cybersecurity Decisions
- Pandemic

The following table highlights the codes and labels emerging from the text:

Table 3.2 Pilot data coding. ***Source****: Compiled by the author.*

Categories	**Sub-categories**	**Empirical data**
Board roles	Oversight	"I've been involved with boards where the CEO is all encompassing, for example in family-owned companies, where the shareholders are aligned to the CEO. Then the board's role becomes more as risk management/ oversight, rather than anything strategic." - Participant 3
	Strategy	"So, were a CEO to use the board, as a sounding board and an advisory role to enhance what objectives the CEO is seeking to achieve, then the board's role becomes not only oversight and stakeholder management - which is common across all boards - but it also becomes very strategic." - Participant 3
Board Behaviour and Dynamics	Formal	"When it comes to the formal board meeting, you know, the quarterly performance, it happens once in three months. You meet along with your private equity (team) and so on." - Participant 1

	Meet frequently	"During Covid times, the three months (meeting) became actually a weekly affair. We used to meet twice a week in the initial weeks or so, but then it phased away. But then you know, as a core team we continued that weekly frequency because we still see that we're not still out of the woods and there is a constant focus which needs to be in place." - Participant 1
Technology Significance and Decisions	Tech acceleration	"So, the technology world is actually going through a massive acceleration and it's almost humanly impossible for 95% of your workforce to keep in step. So, then the problem for - leaders like us, is how do you drive these people?" - Participant 1
	IT mostly centrepiece of business	"Today almost every industry has a very strong technology underpinning whether it's consumer goods or whether it's steel. Every place, technology is just creating massive disruption." - Participant 2
	Many non-tech natives	"Although I'm a part of the (tech) industry, our geekiness is a big problem for the rest of the guys. So, the boards know that this is a big monster, right? But they don't know really what to do or what not to do." - Participant 2
Cybersecurity Factors	Potential for compromise	"The level of ability to compromise through cyber is an exponentially increasing curve... so cybersecurity is one budget which nobody either in the CEO office or the Board has the ability to say no to." - Participant 2
	Industry spectrum	"… the IT industry… and I rank pharmaceuticals similarly. Any highly intensive intellectual property company - even the USB is intellectual property - they were anyway very guarded about any IT risk… because it's still commercial in nature. It is sine qua non for their success, right?" - Participant 3
	Cost vs. investment	"In comparison to yesteryears… it used to be looked at as a cost or expense, absolutely… now it is more looked as an investment. It is being seen, 'I've not spent this much, what is the price of nonconformance?' And we have seen so many cases in recent years - with TalkTalk, with British Airways, with NHS, across the world." - Participant 1

Cybersecurity Decisions	Reputation	"Because it's become a reputational issue and the heightened liability of independent directors under the law, almost every board is now asking what you are doing about cyber." - Participant 3
	Gain business	"For us, this comes in two folds - to be highly secured as an organisation… otherwise we can set a very bad example to our customers, employees and partners. The second aspect is - this is something for us: offering which goes to gain the mindshare of prospects in (a) much better way." - Participant 1
	Compliance	"So, the compliance regime in industry would shape a lot of this and then obviously the nature of the company would also be important." - Participant 2
Pandemic	Work from home	"The difference that the pandemic has caused is the risk that is arisen due to remote working. That's because of security flaws that can arise due to remote working… people are still getting to grips with it. Pre-Covid, nobody had that in mind at all. It was… it wasn't even on their radar. And now it is." - Participant 3
	Augmented work	"So, we had to arrange all those secure networks extended to every individual's home. But manpower is spread across all geography - North America to Canada to Europe to India. To achieve that was a Herculean task and we had to create a task force to create a 24X7 team, to ensure that customers are serviced." - Participant 1
	More attacks	"Covid was unprecedented and none of us had that kind of… exhaustive list. So, you know, the first aspect for us at that point was - how do we retain what we have? Forget about the new aspect, you are talking of retaining it; goes right from employees to customers, to assets, to all the things and cash in the bank." - Participant 1

3.4.6. Pilot Study Learnings

The most significant learnings from the pilot study could be summed up as follows:

- The questions needed to be short and crisp to elicit answers, rather than long and winding, which tended to confuse the participant

- Once a participant started answering a particular question, acknowledging their statements was most productive through facial and body cues – like nodding the head and showing expressions - as opposed to verbal confirmations, which sometimes broke the flow of their speech
- The participants were keen to not share any classified information with the researcher, and once assured that the exploratory themes focussed on their experiences, they were more relaxed toward the process
- As an immediate effect of the Covid-19 pandemic, certain firms were more successful in enduring it than others, and it reflected in the overall comfort and ease of the interviewee in responding to queries
- Certain firms in the technology industry, with adequate focus on and ability to manage enhanced cybersecurity concerns (owing to company resources stretched further than office premises, caused by working from home), were more successful in managing cyber threats
- None of the participants in the pilot study was able to surmise that cybersecurity can be absolutely prepared for, owing to its dynamic nature, with one of them comparing it to fire incidents – it could be prepared for, but needs to be managed if and when incidents occur

These observations were useful in enhancing the researcher's approach to the final data collection. Understanding key points ranging from body language to question flow, all were instrumental in strengthening the researcher's choice of methods, while simultaneously suggesting avenues for improvement.

3.5 Research Methods: Main Study

Insights and lessons learned from the pilot study were instrumental in paving the path for the main study - both in terms of emerging themes for the study as well as methodological finesse. This section describes the aspects of gaining access to corporate elites interviewed for data collection, details of the participants, interviewing them, and analysing the data through thematic analysis, and concerns surrounding researcher bias.

3.5.1 Gaining access

The purpose of this study is to investigate the priority afforded to cybersecurity within corporate strategy, and its advantages to the organisation. Realising that the strategic perspective of cybersecurity may only be realised through conversations with board members and others in the executive committee, elite interviews (Aberbach and Rockman, 2002; Jensen and Zajac, 2004; Harvey, 2011; Mikecz, 2012) with such powerful and privileged interviewees were vital to the study. However, literature has alluded to the challenges of attempting to access, unearth and interpret the black box of board rooms (Watson, Husband, and Ireland, 2020) on account of logistical and practical challenges associated with those. For researchers who are able to access these elites, the consequent challenge is to be able to have authentic and meaningful conversations with such privileged individuals, which makes elite interviewing an enormous challenge (Kakabadse and Louchart, 2012).

As outlined previously, the sampling strategies identified for this research were a combination of purposive (Tongco, 2007) and snowball sampling (Goldstein, 2002), to access the required interviewees. It was crucial to ensure that the interviewees were members of the corporate elite with access to relevant information worth sharing. Furthermore, it was also significant that these participants represented a wide range of industry sectors to present a holistic understanding of the cybersecurity strategy in organisations. In keeping with the same objective of a holistic understanding, it was also key to explore both public and private sectors, as well as individual consultants providing cybersecurity expertise to larger organisations. This was a useful strategy to gain access to these participants who, pleased with the interview themselves, were able to offer access to others in their network, demonstrating snowball sampling in practice.

A challenge posed to the above strategy was the sudden onset of the Covid-19 pandemic, as organisations were grappling with severe challenges ranging from security to survival, thus relegating participating in a research exercise to the low end of their priorities. As having a specifically characterised sample to interview was vital to maintain the integrity of the data, the *purposive* nature of sampling was not interfered with. However, the *snowball* aspect could not be relied upon in its intended sense. Observing the world gravitate towards 'the virtual' seemingly overnight, a significant aspect of this access to the interviewees was through the virtual network of LinkedIn (Dicce and Ewers, 2020). The researcher scoured it for board members with relevant background and experience and contacted them through LinkedIn messaging.

Another challenge is posed by the numerous gatekeepers (Mikecz, 2012) surrounding these participants, who screen the individuals demanding the time and attention of such elites. To overcome this challenge, the researcher contacted their professional network (from a different geographic location) to gain access to their counterparts within the UK, to identify and discover other willing and suitable participants. Besides this, support was sought from interview participants among consulting agents, to allow access to their networks, in turn - further developing the *snowball* aspect of finding suitable participants. This was a helpful methodological choice, as elites with rigorous time schedules (Mikecz, 2012) may be unwilling to trust the researcher, consequently leading to non-response to interview/participation requests (Goldstein, 2002).

Through each of the sampling choices, a letter was thoughtfully crafted explaining the purpose of the interview, information about use of data, clarification regarding ethical choices having been approved from necessary authorities (University of Reading Ethics Committee), and the value of the interview to the research and business community overall (see **Appendix 1**). Since the interviews were conducted during the ongoing Covid-19 pandemic, these were planned as recorded video interviews (Archibald *et al.*, 2019; Gray *et al.*, 2020) through Microsoft Teams, for ease of consequent transcription. The above letter, thus also functioned as a consent form for the video recording of the interview and the information being conveyed, besides explaining the ways the information would be collected, stored, and eventually destroyed after a given time.

3.5.2 Main Study Sample

The final sample comprised of 31 participants belonging to different industry sectors and at high-level positions, as necessitated by the requirements of the study. The sample was developed with a balanced combination of participants from the personal network of the researcher as well as those referred by other participants. Some of them held prestigious titles such as Knighthood and OBE (Order of the British Empire). These participants also represented a healthy divide between the board members and the executives with a 52% and 48% split, respectively. This representation is vital for the study, as cybersecurity strategy creation and implementation are both significant aspects for a successful cybersecurity policy. This is thus governed and managed together by the governing board and their executives. Furthermore, while the gender of the participant was not a factor considered for this study, 22% identified as women. This highlights the challenge of presenting a balance of genders between participants yet is a figure representative of the rising female prominence amongst the UK-based corporate elite.

*Table 3.3 Participant details. **Source**: Compiled by the author.*

S. No.	Gender	Board/Executive	Industry Sector	Sampling Reference
1	Male	Board member	Engineering	Personal network
2	Male	Executive	Technology	Personal network
3	Male	Board member	Education	Personal network
4	Male	Board member	Engineering	Snowball
5	Male	Board member	BFSI	Snowball
6	Male	Board member	Consulting	Personal network
7	Male	Board member	BFSI	Personal network
8	Male	Executive	Consulting	LinkedIn
9	Male	Board member	Technology	Snowball
10	Male	Executive	BFSI	Snowball
11	Male	Executive	Technology	Snowball
12	Male	Executive	Technology	Snowball
13	Female	Executive	Consulting	LinkedIn
14	Male	Executive	Consulting	LinkedIn
15	Female	Board member	Service Provider	LinkedIn
16	Female	Executive	Technology	LinkedIn
17	Female	Executive	Consulting	Snowball
18	Male	Executive	Technology	Snowball
19	Male	Executive	Consulting	Snowball
20	Male	Board member	BFSI	Personal network
21	Male	Executive	Service Provider	Snowball
22	Female	Executive	Defence	Personal network
23	Male	Board member	Defence	Snowball
24	Male	Executive	Defence	Snowball
25	Male	Executive	Govt.	Snowball
26	Male	Board member	BFSI	Personal network
27	Male	Board member	Consulting	Personal network
28	Female	Board member	Govt.	LinkedIn
29	Male	Board member	Govt.	Snowball
30	Female	Board member	BFSI	LinkedIn
31	Male	Board member	Govt.	Snowball

With respect to the industry sectors the participants belonged to or primarily represented, the same is presented in **Table 3.4**. The tabulated figures demonstrate 19% hailed from the different divisions of the technology sector. Another 19% represented the banking and other financial services industry. 22% engaged in the consulting industry, including cybersecurity, governance, and management consulting. One each among the participants belonged to the education, transportation, internet service provider industries. Roughly 10% of the sample interviewed was from the defence industry, which understandably confers an increasing priority to cyber-defence. Public sector and/or government was the industry comprising 13%

of the sample. Engineering and manufacturing, which is similarly growing its reliance on digitisation, was the industry for 2 of the sample participants. However, it may be useful to note that some of the participants were also independent board directors, thus representing other industry sectors not necessarily highlighted here. Similarly, the participants' previous roles also belonged to industry sectors other than the ones they represented during the interviews. However, this prior experience, and sometimes expertise, was crucial for framing their understanding of the cybersecurity strategy and associated concerns explored by this research.

Table 3.4 Industry sector split in participants. ***Source****: Compiled by author*

Industry Sector	**Number**
Technology	6
Engineering and Manufacturing	2
Banking and Financial Services	6
Education	1
Defence	3
Transport	1
Consulting	7
Public Sector/Govt.	4
Internet Service Provider	1

3.5.3 Elite Interviewing

As is often customary in literature, there are varied perspectives for the term 'elite' - ranging from 'ultra elites' to 'professional elites' (Harvey, 2011). However, for the purpose of this study, members of the executive committee and board members are, together, considered elite with respect to their influence in cybersecurity decision-making, as well as their experience in the field.

As pointed out previously, gaining access to and holding meaningful conversations with corporate elites is made challenging for a number of reasons. Firstly, on account of their rigorous time schedules (Mikecz, 2012), it is both difficult to access them and seek an adequate amount of time with them to have a productive discussion for the study. Secondly, gaining their trust (Harvey, 2011) is another uphill task, as that involves ensuring trustworthiness as a researcher, while demonstrating authenticity and importance of the research so as to motivate them to engage in an interaction. This was of particular significance with this study, as cybersecurity concerns (including but not limited to past cybersecurity incidents - both big and small) are often considerably guarded information. Seeking the help of gatekeepers (who provided references), maintaining high ethical standards of the study and an objective aimed at benefiting the business community at large, as well as adopting a conversation-like tone of the interview, helped develop their trust.

Another challenge is also created by those potential participants willing to have an interaction with the researcher, yet unavailable at the given time of the data collection, which sometimes results in non-response bias (Goldstein, 2002). This caused considerable consternation to the researcher as the changing global scenario (impacted by Covid-19), in general, and worsening cyber domains of organisations, in particular, were beyond the control/influence of the researcher. The primary course of action was to persist with other potential participants (which was certainly useful) or, in certain cases, to stay patient and wait for the initial participant to find an opportunity to have the said interaction.

However, once participants managed to take out time for the interviews, it was incumbent on the researcher to be adequately prepared for the conversations with them. This was particularly useful in cases when some interviewees were inherently laconic or otherwise unmotivated to share copious amounts of information with the researcher. Thus, good preparation helped in having comfortable conversations with the participants, as well lending credibility for future interviews (Goldstein, 2002) and being referred to others in the participants' networks. This was of considerable help in this study as the imbalance of the power dynamics between the corporate elites and academic researchers may sometimes negatively influence the information exchange in such interactions. Similarly, open-ended questions leading to a conversation, rather than a supposed interrogation, promotes a continuing interaction, which is not leaning strongly on a sequence of questions and being referred to them (Aberbach and Rockman, 2002).

Thus, though challenging in certain respects, the initial few interviews coupled with adequate reference to literature, provided enormous insights into the development of a unique yet authentic interview style which facilitated information-sharing by the elite participants.

3.5.4 Data Analysis

The analysis of data collected through this study was analysed through Thematic Analysis - as highlighted previously in section **3.3.9.5**. The following sections describe the components involved in understanding and analysing the data, which enabled generating findings from it, which is further explained in the next chapter.

3.5.4.1 Transcription of Interview Data

The interview durations were within the range of 30-120 minutes, with a majority lasting for 65 minutes. As mentioned previously, these were conducted on Microsoft Teams, which facilitated a recording of the interview (with participant consent) on Microsoft One Drive, available with a closed-captioning feature provided by the software. Microsoft, being the university-approved and subscribed-to software, was the video conferencing software of choice. Similarly, the Microsoft One Drive was approved by the university to record and manage the interview in a virtually protected location, with only access to the researcher - which enabled the security and data integrity.

While transcription has been understood to help researchers interpret interviewee experience and perceptions (McLellan, MaCqueen and Neidig, 2003), literature supports the importance of the way the content is heard and transcribed, as well (MacLean et al., 2004). Thus, it is important to highlight that the entire data collected through interviews was transcribed by the researcher. (A sample transcription file is available to view in **Appendix 3**). Though some basic form of closed-captioning was provided by the Microsoft Stream software, it unfortunately, was not reliable as it was peppered with errors - owing to differences in the participants' pronunciation, tone, voice modulation, accent, etc. The following subsections describe the significant elements of the data analysis thus transcribed.

3.5.4.2 Applying Thematic Analysis

Analysis of the data, using thematic analysis for this study, was conducted in 6 states which, while seemingly linear, also incorporated several iterations: first between steps 2, 3, and 4; and later between steps 4, 5, and 6. This process has been highlighted in the adjacent **Figure 3.2**.

The description for each of the steps is as follows:

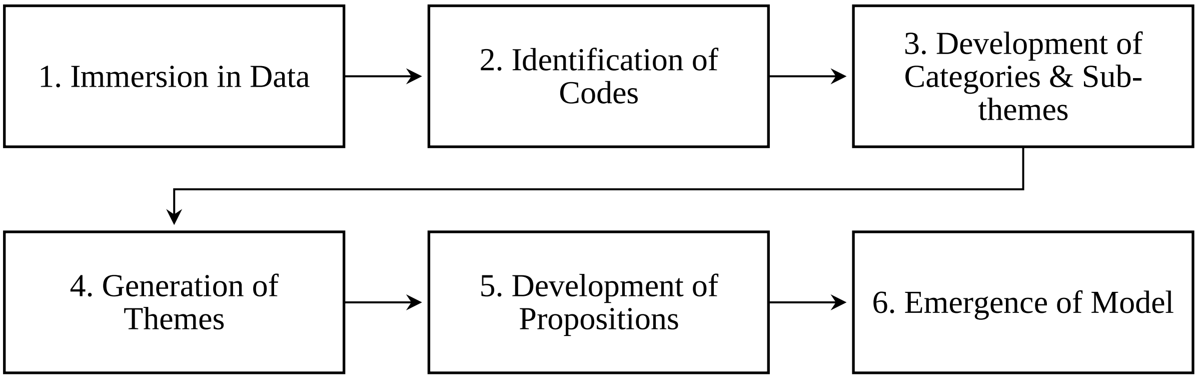
1. Immersion in Data
2. Identification of Codes
3. Development of Categories & Sub-themes
4. Generation of Themes
5. Development of Propositions
6. Emergence of Model

*Figure 3.2 Thematic analysis process. **Source**: Compiled by the author.*

i. *Immersion in data -*

This stage commences the data analysis process with thematic analysis aimed at becoming intimately familiar with the data. For this purpose, the transcripts were read through several times and annotations were frequently marked each time some important/useful keyword or information was identified. These were viewed in two ways - one being those instances which the interviewee believed were significant, or distinctive, or repeated through the course of the interview, or led to other information being uncovered. The other was those identified by the researcher to be often important or other key pieces of information shared by the participants. These annotations were vital to understanding the hallmarks of each interview transcript and were viewed as unique identifiers. Other studies investigating governing boards have employed similar procedures (Kakabadse, Kakabadse and Barratt, 2006), which reinforce the use of this mechanism.

Together, these annotations lead to the identification of first-order coding, which is the next stage.

ii. *Identification of codes*

This is the first stage in identifying meaningful units which have been labelled individually from the transcribed data. In the example of Theme 1, which is demonstrated in the **Figure 3.5**, the first order of labelling identified 30 distinct codes which were vital to the eventual development of themes. This stage is synonymous with the open coding stage highlighted by Strauss and Corbin (1990).

The codes thus identified led to the next stage, described below.

iii. Development of categories and sub-themes

At this stage of the process, the relationships between the codes identified in the previous stage are drawn out and presented in a hierarchical form. In the example highlighted in the adjacent **Table 3.5** for Theme 1, 5 categories were developed through the 30 codes identified together in Stage 1. Here, the 3 key categories explaining the relationship between the 13 codes led to the development of a sub-theme - 'Organisational characteristics impacting cybersecurity needs.' Similarly, 2 other categories led to the next sub-theme - 'Organisational decision-makers for cybersecurity'.

These 2 sub-themes further led to the generation of themes in the following stage.

iv. Generation of themes

Themes were generated at this stage from the exploration and refinement of the sub-themes which emerged at the previous stage. This stage is synonymous with the selective coding outlined by Strauss and Corbin (1990). Using selective coding, similar to grounded theory approach, has been incorporated in similar studies investigating corporate boards (Kakabadse, Kakabadse and Barratt, 2006). To explain with the help of one theme, for instance, **Table 3.5** demonstrates the development of Theme 1 from the two sub-themes. Here the underlying commonality highlighted the importance and subjectivity of each organisation that set out to create its cybersecurity strategy. The combined list of factors involved here further influenced the ways in which each organisation operationalised its cybersecurity strategy and highlighted its success with respect to its competitors.

Once the themes were generated, the next stage followed.

v. Development of propositions

With the generation of the themes and their sub-themes, the significant inter-relationships were subsequently made evident, which enabled the development of propositions to be empirically tested in the future. This led to the final stage of the process, which is the next step.

vi. Emergence of model

This was the penultimate stage of applying thematic analysis, wherein the developed propositions led to the construction of a model explaining the factors which lead to the creation of cybersecurity strategies which afford the organisations certain opportunities - including competitive advantage. This is described in detail in **Chapter 5**.

Table 3.5 Stages of theme development. ***Source****: Developed by the author.*

CODES	CATEGORIES	SUB-THEMES	THEME
CS is technology/security	CS Perspective of Org	Organisational characteristics impacting CS needs	*THEME1* Organisation
CS is People-Process-Tech			
CS is physical, digital, and social			
CS is risk			
Code of Conduct	Ethics in Tech		
Misuse of tech			
Society at large ethics			
Sectors of org	Organisation characteristics driving CS needs		
Size of org			
All orgs need CS			
Competitor driven factors			
Customer data driven factors			
Other org characteristics driven			
Role of Board	Board Characteristics	Organisational decision-makers for CS	
Board composition			
Board tech expertise			
Board meeting frequency			
Board risk perception			
Board priority to CS			
Board budget for CS			
Boards forced to prioritise CS			
Board duties	Decision makers for CS		
Executive duties			
Best case scenario			
Outsourced help in CS			
Somebody else decides			
Board/Exec depends on?			
Committee for CS			

3.5.4.3 Researcher Bias

For a qualitative study employing an inductive enquiry logic as elucidated in **3.3.2,** there is a probability of researcher bias being inadvertently employed. This study explores the cybersecurity strategy for organisations and their potential to lead to competitive advantage, and thus any bias would be unfortunate. However, following an interpretivist philosophical position, as described in **3.2,** the researcher is part of what is being researched and thus cannot be separated from the subject (Saunders, Lewis, and Thornhill, 2009a). Furthermore, efforts were employed to ensure academic rigour to the research design, such that the researcher bias would be reduced to a minimum. Moreover, strict personal and professional ethical standards - aimed at maintaining the intentional meaning and context of information shared - were similarly adhered to.

3.6 Chapter Summary

Cybersecurity is a momentous cause of concern in the ever-changing digitalised world of today. Swift advances in the field of technology have brought with them an elevated level of uncertainty, which could be construed as both a reward and a penalty. This uncertainty can have a major impact on the competitive position of companies and, thus, warrants strategic attention (Elahi, 2013). The governance of cybersecurity does not merely apply to the management of threats; rather, it extends to ensuring having a framework in place under which all future potential threats could be readily addressed, with a top-down approach. Critical to this study is to determine how cybersecurity is integrated, or not, into the company's strategy-making by uncovering how directors exercise their roles. This way, the governance of cybersecurity will be positioned not only as a management of threat but also as the realisation of competitive advantage captured in the daily activities of directors.

CHAPTER 4:
Data Analysis & Discussion

4.1 Introduction

This chapter discusses the themes as they have evolved through the analysis of the extensive data collection, as discussed in the previous chapter. The interviews have uncovered insightful perspectives about the inner workings of the organisational path to crafting their cybersecurity strategy. Each organisation’s choice of cybersecurity strategy is influenced by their organisational/ industry characteristics which further impacts how they respond to the range of challenges they encounter. The way they overcome these challenges, draw insights from them, and inform their future choices, influences the advantages they gain from a robust cybersecurity system. This chapter, therefore, articulates the process which has led to the emergence of themes and sub-themes, which together lead to the development of a model explaining the framework, which this thesis makes as a contribution to the realm of cybersecurity governance.

4.2 Theme Development

This chapter discusses the five main themes which have emerged from the in-depth interviews. To begin with, it covers the collection of organisational characteristics which strongly influence the organisational stance on cybersecurity. This includes both the characteristic features of their decision makers, along with a host of other organisational features which determine their path to cybersecurity strategy and its robustness, or lack thereof. It then discusses the various challenges that befall organisations as they try to implement a robust cybersecurity strategy. These challenges are broadly covered under two sub-themes of cybersecurity incidents and macro-economic challenges. Moving ahead, the chapter then explores the implements used to confront the challenges thus discussed. These tools are broadly covered under three sub-themes of board engagement levers, insights, and regulation. Each of these three sub-themes supports the implementation of robust cybersecurity governance mechanisms. Following that, the advantages of a fortified cybersecurity system are discussed, which are then divided into potential competitive advantage and organisation specific advantages. The final theme of winners is then explained in detail, with the characteristics of ‘winners’ being discussed. Each of these themes is supported with quotes from interviewees to support the emergence of themes and sub-themes.

The following table clearly outlines the themes which emerged through thematic analysis of data. The tabulation of themes and sub-themes enables ready comprehension of the significant outcomes of analysis, which are further discussed through direct quotes from participants and supporting literature for each theme and sub-theme, consequently.

Table 4.1 Summary of themes. ***Source****: Developed by the author.*

Themes	**Sub-themes**
4.3 Theme 1 Organisation	4.3.1. Organisational characteristics impacting CS needs 4.3.1.1 CS Perspective 4.3.1.2 Ethical Point of View 4.3.1.3 Organisational Features 4.3.2. Organisational decision makers for CS 4.3.2.1. Board Characteristics 4.3.2.2. Final Decision makers
4.4 Theme 2 Challenges to Attaining Robust CS	4.4.1. CS Incidents 4.4.2. Macro-economic Challenges 4.4.2.1. Pandemic 4.4.2.2. Industry Level Challenges 4.4.2.2.1. People Challenge 4.4.2.2.2. Technology Acceleration 4.4.2.2.3. Criminal Motivation/ Access 4.4.2.2.4. Big Market for CS Products
4.5 Theme 3 Tools for Confronting CS Challenges	4.5.1. Board Engagement Levers 4.5.1.1. Risk Associated with CS 4.5.1.2. Costs Associated with CS 4.5.1.3. Inhibitions Around CS 4.5.2. Insights 4.5.2.1. Correct Board Language

	4.5.2.2. People-Processes-Technology 4.5.2.3. Elementary Realisations 4.5.3. Regulation
4.6 Theme 4 Advantages from Robust CS	4.6.1. Competitive Advantage 4.6.2. Organisation Specific Advantages 4.6.2.1. Trust 4.6.2.2. Reputation 4.6.2.3. Business Growth
4.7 Theme 5 Winners	4.7.1. Winners

4.3 Theme 1: Organisation

‘Organisation’ is the first theme which emerged as a consequence of analysing the invaluable information shared by the interviewees. While the unit of analysis was these individuals, the impact of cybersecurity strategy - both successfully and inadequately - was experienced at the organisational level. This theme explores the shared factors between organisations on their path of robust cybersecure realms. These are divided into two sub-themes - the first associated with the organisation, its industry sector, and the organisational chosen perspectives which influence their subsequent cybersecurity decisions, and the second relating to the decision makers in each organisation, including the governing board directors and the executive team. These are explained in the following sections.

4.3.1 Organisational Characteristics Impacting CS needs

Organisational characteristics are the primary features impacting the needs and, consequently, the mechanism an organisation ensures for securing its cyber domain. In the larger scheme of things, they together influence the way an organisation perceives the significance of technology, its cyber space, and the need to safeguard its cumulative assets. The following three sub-themes describe these.

4.3.1.1 CS Perspective of Organisation

Cybersecurity perspective is at the heart of the organisation, it even crafts the strategy to protect the organisation's cyber realm. It particularly gains significance as cybersecurity is often perceived to be highly technical in nature, and sometimes even limited to the technical domain or an IT problem (Kosutic and Pigni, 2020). This perspective of viewing cybersecurity from more than a mere technical perspective certainly has its advantages. Research has pointed out that a technical viewpoint for cybersecurity is a limiting one, exposing its potential threats and vulnerabilities (Boyes, 2015). It may even be considered 'myopic' (Sallos et al., 2019) as it fails to account for all the various other perspectives which underpin its successful management.

In cases where the organisation's perspective on protecting its cyber spaces is limited to technical areas, often their Information Technology (IT) department is responsible to make the vital cybersecurity-related decisions. Increasingly the conversations with the participants raised the understanding that for cybersecurity to be competitive, it needs the attention and focus of the top its corporate pyramid, following a top-down approach (Hubbard et al., 2021). Having, then, only the IT team bearing the burden of cybersecurity mandate, limits its effectiveness and potential. Thus, how an organisation viewed cybersecurity, and their respective interpretations of it, often defined the importance it experienced in their strategic agenda.

Many participants voiced that, according to them, cybersecurity was an extension of their organisation's view of the risk it encountered. Viewing it, then, as a risk meant that their actions associated with cybersecurity were conducted considering the implications and costs surrounding it. Studies in recent times increasingly mirror this approach within the practitioner community. Nolan, Lawyer, and Dodd, (2019) highlight one of the best ways to ensure the importance of cybersecurity in the boardroom is to quantify it in financial terms. According to them, managing cybersecurity can be done with a top-down approach - just like any other business risk - by associating a business value to its cyber-risk. This further supports the perspective of viewing cyber concerns as risks to the business. One of the interviewees was of the opinion that,

"A large chunk of the board's time needs to be spent talking about how the risk environment is changing around them. And fitting into that is - what is the risk to your business's delivery strategy from cyber space? So, if for example, if you were going into China, you'd be thinking, 'Well, yeah, I need to really think about what does this change about my business's risk profile

- does it make me more attractive to fraudsters? Does it make me more likely to see an exponential increase in malware attacks? How do I train my employees better to then be able to spot those risks, and minimise the chance of losing data?'" - Participant 28

It may, then, be understood that the perspective of cybersecurity is decided in terms of the risk to achieving business objectives in the cyber realm. Approaching it, in that sense, will allow an organisation to have the right conversations, which then drives the processes for the apt cyber strategy required to deliver on its strategic objectives. Empirical studies also support the increasing practitioner behaviour wherein governing boards are citing cybersecurity concerns as their primary risks (Landefeld, Mejia and Handy, 2015) .

This was further mirrored in the interviews where one participant emphasised the importance to perceive it not as a technology concern, but as an issue from a risk-based perspective. They voiced the following opinion,

"I think, ultimately, the most important thing is not the technical approach, I dare say it. And actually, the most effective way that any organisation, any structure, can secure itself is really looking at it from a risk-based perspective." - Participant 27

Finding this response also formed curiosities regarding the importance of viewing it from a technology and/ or security perspective. A large number of participants fused the two together instead of choosing one over the other, which confirmed it as a viable perspective of many organisations on cybersecurity. One of the participants was keen to explain the cybersecurity needs to be viewed from a balanced perspective of both technology as well as security, in order to be able to organise it appropriately. One or the other is a limiting view, and they explained their reasoning for coupling technology and security together in the following words,

"So, on the one hand, you do need to have a good understanding of the technology and its vulnerability in order to be able to apply good security across the board and deploy good cyber security strategy - which addresses the needs of the business - and then decide what technologies are needed to be deployed, to keep it safe. On the other hand, the security awareness aspect of it is super important. You can't be just good at one or the other because focussing purely on the technology won't help you. So, providing significant enough technical interventions in order to secure the network is also important." - Participant 25

Another common perspective was to move beyond the digital idea of cybersecurity and incorporate the physical element with it. This way of thinking is also supported in research - termed as ‘defence in depth’ - citing the advantages of strengthening physical security, which further aids cybersecurity (Barnes, 2019). This essentially, is a clear choice to realise - that while cybersecurity is aimed at safeguarding an organisation’s cyber assets, the security itself involves firstly safeguarding the physical assets associated with the cyber realm. One of participants clarified this point through the following words,

“This is why we were saying cyber security doesn't work on its own. So, if you need to think about the physical security and all of that, because the cyber security is focussed on the digital, the question arises, ‘Why would I waste my time trying to break your network when I can literally just go through the front door?’” - Participant 16

While it may seem simplistic, it underscores an essential learning from the field. For a border-less entity such as the cyber realm, limiting it to the actual digital space would be an oversight with potential to cause considerable damage. This view of coupling the digital and physical world, allows cybersecurity to have a more robust perspective, thereby limiting potential for vulnerabilities.

Others were able to have a more holistic view of cybersecurity instead and believed that the perspective owed to cybersecurity demanded a broader view incorporating the people involved, the processes outlined, and the technology it is all based on. According to them, this perspective was useful in preparing adequately for strengthening the organisational cybersecurity governance. One of them articulated their point thus,

“There's obviously a lot of un-targeted or non-targeted malware that just sits, and then you've got the targeted malware… but I think in terms of overall cyber hygiene and the way we have these - processes, people and technology approaches - that's just equally important for an organisation to concentrate on and not just think about what the major threat actors are doing.” - Participant 27

All the above opinions may vary in the way they viewed cybersecurity itself, however the commonality they shared was viewing it from more than a technological perspective. Cybersecurity conversations with a technological lens are often limiting in the attention the topic deserves and, consequently, the resources which are diverted to it. So perhaps, it would be beneficial to organisations to widen their scope and offer it the gravity it commands. The next subsection explains another organisational perspective, which consequently informs their stand on cybersecurity as well - ethics in technology.

4.3.1.2 Ethical Point of View

It is intriguing to note that often an organisational choice, from its cybersecurity standpoint, is also influenced by its ethical perspective on technology as a whole. This is a testament to the growing conversations centred around corporate responsibility related to the organisation's digital or cyber realm, increasingly being referred to as the Corporate Digital Responsibility (Lobschat et al., 2021). Considering this, perhaps not differentiating the more successful from the less successful, but certainly their choices (guiding the fortifying of their cybersecurity realms) could be related to the chosen view of ethics associated with technology as well. For instance, an organisation that appreciates the significance of their end customer being able to experience products/ services with in-built secure software and operating systems will more often be one that values cybersecurity as well.

One of the interviewees had a helpful view which associated winning the customer's trust with an ethical viewpoint, which may be viewed as a precious resource for the organisation to possess. Their stance was clear in stating that viewing it from an ethical perspective, enables an organisation to secure the customer's trust which is important in growing business - especially as customers trust businesses to protect their information (Wright, 2021) they seek from them. They articulated their thoughts, saying,

"I think that's where the emphasis needs to go full circle in terms of the business perspective. Whatever service, whatever it is I'm selling, whatever I'm putting in the market, I would then have a duty of care – to whoever buys that service - to have a baseline level of security and what you have done to help. And then I say it's all about trust. So, you're kind of saying it's really important that I don't just give you this product with no security whatsoever." - Participant 16

Such a view would then invariably involve the organisation ensuring the customer's security, as well as laying it as a foundation for the organisation itself. Practitioner reports confirm that organisations are increasingly being urged to incorporate ethical principles (Cisco and affiliates, 2023), especially when using modern technologies like AI. Another view that took this ethical viewpoint a step further was the justification that this smaller step led to the larger good of society, which was implied as a preferred objective that organisations ought to strive for.

A participant opined the following thought which, from a shareholder perspective, may be considered not the priority. It is supported by research which maintains that this ethical behaviour may not allow firms to maximise sales and profit (Bleier, Goldfarb, and Tucker 2020; Hagendorff 2020). However, perhaps that was an underpinning notion which garnered attention, as the focus should not be restricted to just the shareholders but all the other stakeholders as well, which translates to thinking beyond just profit.

"So, I think that technology, for lack of a better word, has to have a better moral compass. We understand the full impact of what technology can and cannot do, and to accomplish this result we have to factor in what security is needed. And yes, that might affect my bottom line, but overall, if we're using tech responsibly, it makes society stronger, so there's a qualitative result, not just quantitative – meaning, more money for the stockholder centres." - Participant 14

Another viewpoint which gathered considerable importance within the ethics employed (or lack thereof) within technology was the insistence on requesting considerable customer information, when it may or may not be required, for the sale of the product/service. It is often found that the technology behemoths which dominate the industry demand this information from the customers, who then have but little choice in the matter. Contemporary research is highlighting the concerns raised by this practice (Andrew and Baker, 2021; Bleier, Goldfarb, and Tucker, 2020; Martin, 2015). One of the interviewees had strong views on the matter, saying,

"So, when I'm a Google or Facebook and I have someone that's on my platform, I'm taking a lot of things - information preferences and I'm using this information to then kind of influence things and that has a high value to businesses… I guess it's beneficial for big tech, but it's not a healthy relationship for the end user. So, I'm more aware, I'm going to make some changes with how I use tech. And through these changes, I will affect the partnership that I want to have, and I will dictate that partnership. So, the relationship is healthy and mutually beneficial." - Participant 14

Studies are increasingly exploring the ethical trade-offs when crafting effective cybersecurity practices, even going as far as recommending ethical frameworks on which to construct an ethical cybersecurity practice (Formosa et al., 2021). One of the participants from the study had related views from the organisational perspective, questioning the need for information from the customer which in no way affects the sale of the product or service from the organisation.

"One of the arguments that keeps happening with some of the design guys or the product guys, or the business guys is, 'Oh, can we capture this?' 'That's fine, but what are you going to do with it?' 'But we need it.' 'For what? There's no point in storing it if you don't need it, right?' If it never comes out the other end and is not used for anything, why am I asking for it? And this goes back down to the design and the user experience. Just ask for stuff that you really need. If people will just ask 'cause we can, yeah well you can ask for anything but, people get fed up if you ask stuff that is (of) no value." - Participant 10

In a linear fashion, the more information the organisation collects, the more the cyber exposure as vulnerabilities, and consequently more volumes of data/ information to safeguard and protect. While regulations like GDPR hold organisations accountable (Kiesow, Cortez and Dekker, 2022) for such information (Michael et al., 2019), perhaps an ethical viewpoint towards the collection of stakeholder information, as well as providing secure end products to customers would enable organisations to reduce their cyber risk exposure. For any benefit to accumulate from that, however, such ethical choices have to be made much in advance. The next subsection explores the other organisational factors which impact the way an organisation's cybersecurity needs are defined.

4.3.1.3 Organisational features

This category incorporates several organisational features which would influence their consequent choices with regard to cybersecurity governance. Some of those features, for instance the industry sector - like technology sector - necessitated their observing strict cybersecurity measures. In other instances, the organisational size had a direct impact as, understandably, larger organisations with more information and stakeholders are compelled to incorporate robust and often state-of-the-art cybersecurity protection.

The digitalised era of the 4.0 economy is characterised by the merger of product and process data with machine data, enabling the interconnection of and communication between machines (Corallo et al., 2020). Here, a popular way to embrace this perspective is that all organisations, across sectors, irrespective of their size, or stage in life cycle, heavily relied on technology for their essential functioning, and therefore were not offered an option but to safeguard all parts of the organisation supported by technology.

"I think that with something like cyber security, all companies have that requirement, as it's kind of just part of doing business. Whatever industry they're in, even if they run a shop, there's technology running around that has to work. So, I think that it's definitely something that's very important." - Participant 13

Similarly, another participant elaborated on this view, explaining that technology underpins most business functions which may make them view themselves as technology organisations. In such cases, it is thus important to prioritise securing their technological assets, with the following thoughts,

"Many companies now see themselves as technology companies, even though their service could be finance or pharmaceuticals or retail; the technology is what underpins everything. Traditionally cybersecurity is being around protecting infrastructure. But we're not protecting infrastructure, we're protecting data, we're protecting the information, we're protecting the assets, we're protecting the people. But you know the technology that underpins everything, as we sort of said, is becoming so ingrained in everything that you can't just look at cybersecurity on its own." - Participant 16

A related viewpoint emphasised the significance of data/information collected by most organisations (Kiesow, Cortez and Dekker, 2022) which made it necessary for tough cybersecurity measures to ensure that while the data itself was secure, along with the organisations that were being interconnected through it. This could range anywhere from banks (Wright, 2021), to retail businesses, to even automobile and/or firms in the hospitality industry. Their thoughts were,

"Well, if you're handling a lot of personal information, you have got to take this seriously. You just can't afford to ignore it 'cause you will lose it." - Participant 31

Some others were keen to highlight certain sectors which invariably were the focus of threat actors in the cyber realm, and therefore needed to be proactive with their cybersecurity regimen. Empirical studies from practitioner experience increasingly point to the significance of protective and proactive aspects (Hubbard et al., 2021) as well. Reflecting the logical understanding of those industries which either rely on customer data for functioning or on technology for revenue, these industries are then expected to be more cyber-conscious than their counterparts in other industries. Nolan, Lawyer, and Dodd, (2019), amongst other researchers, support this view while highlighting the need faced by organisations in healthcare, transport and logistics, power generation, and others. One of the interviewees pointed out these sectors, saying,

"We can wrap them around the critical national infrastructure (CNI). Financial services is one of its kind pillars; telecom sector is another one. These are the organisations that need commercial-oriented cybersecurity, where vendors will probably not be able to provide fool-proof security because the threats and the risk posture for these CNI entities is very different from, let's say, a leisure company, for example. So, the risks are different, the threats are different, and it needs a very in-depth and up-to-date understanding of how those cyber threats are evolving." - Participant 22

A sector persistently targeted by criminals is the financial sector which includes banking and financial services like insurance. While it was robbery in the previous decades, the setting of crime in current times is increasingly in the financial organisation's cyber-space (Nicholls et al., 2021). The motivation could range from direct economic gain to illicit use/sale of the data stolen from the financial enterprise. Similarly, the technology sector is another one which relies heavily on technology, which necessitates its priority to acquire robust cybersecurity. Alluding to the *logic of appropriateness* (Wessels et al., 2021), technology companies often invest in appropriate cybersecurity measures. This relates to a commensurate level of effort and investment in cybersecurity, as necessitated, rather than a fixed degree regardless of the circumstances. Another participant clarified this idea with,

"We've recently seen some very large nation-states' cyber-attacks and, clearly, SolarWinds was one. Ultimately when you look at who were the targets, the tech companies were - because you know if you compromise one of these technology companies, you can get to all of their clients. I think it's been a wake-up call the last 12 months for tech, seeing how they are such a high-priority target, and I think we will start to see more and more products prioritising security." - Participant 29

Another sector which struggled with maintaining high standards of cybersecurity was highlighted as the public sector, which has been known to be under-funded unlike the private sector, where access to resources is not similarly restricted. This was voiced by one of the participants, saying,

"I think public sector (organisations) are very vulnerable because of a lack of funding. Fundamentally, you know if your primary source of funding is meant to be spent on delivering a public service, then that's what you're held accountable for. Not held accountable for investing X millions of pounds in a security information and event management platform, because the public doesn't care. The public only cares when all their personal data is found online." - Participant 21

Other interviewees also attributed the organisation's size to the impact on its cybersecurity needs. A few believed that larger organisations, with access to more resources (both financial and human), were able to access better cybersecurity governance mechanisms, consequently. In contrast, those smaller or even medium sized organisations, while aware of their cyber vulnerabilities, were not able to access these. They either lacked the financial means to implement adequate cybersecurity measures or did not possess the personnel needed to affect such measures (Wessels et al., 2021). One of the participants found an amusing analogy to explain this, saying,

"So, inevitably budget for this type of thing is a factor - without a doubt. We've also seen some people come in inquiring about services and I've had it described as looking for a 'champagne service at a beer price.' Sometimes their expectations are just not realistic. But you know there is a cost to data security and data privacy, without a doubt." - Participant 8

These were most of the thoughts associated with organisational features impacting the need for stronger cybersecurity measures, and the associate literature supporting them. The next subsection looks at the decision-makers in an organisation who are largely understood to influence the organisation's choice of cybersecurity stance.

4.3.2 Organisational Decision-makers for CS

While speaking to the interviewees, their views on the decision-makers for their respective organisation varied between the chief executive team, the board, and sometimes the committees formed to oversee the cybersecurity-related matters. It is understood that the operational strategy of running the organisation day-to-day is configured by the executive team, with advice from the governing board, which scrutinises each element of the strategy. This includes the cybersecurity strategy as well. However, depending on the organisation itself, there were two main factors which were highlighted within these, which bear a closer look.

4.3.2.1 Board characteristics

Overall, the board characteristics have begun to display changes with respect to the growing significance that cybersecurity has garnered in recent years. Sometimes, these changes have been palpable through the changes to board composition, while at other times these changes have been to the skill set and/or expectations from the board members. Research underscores the significance of IT expertise in governing boards to performing oversight responsibilities (Landefeld, Mejia and Handy, 2015) associated with cybersecurity (Hartmann and Carmenate, 2021) governance. The unifying factor across is the need for a more cyber-aware board (Cerin, 2020) which is equipped to manage and govern the organisation's cybersecurity landscape.

One of the interviewees pointed out the importance of board significance with respect to their diverse backgrounds and perspectives, which brought robustness to all discussions and decision-making, including that of cybersecurity. They pointed out,

"I see a big difference when I'm a lone voice on the board versus (when) I'm one of three or four on the board who think differently. So yeah, composition is massively important. It's not to say that you're not going to succeed with ... You can manage all of them, but it just feels as though you get quicker to the right answer with certain compositions of a board than you do if it's all like-minded thinkers." - Participant 15

Once again, with cybersecurity being easily perceived as a technology-related subject area, the technological skill set/qualification of the board members comes into focus. Academics have highlighted this, emphasising the combined expertise in IT and cybersecurity in boards is fairly limited (Gale et al., 2022; Hartmann and Carmenate, 2021). Especially because, ordinarily, most board members have decades of experience prior to the generation that is popularly known as 'technology natives' - those born into and who associate comfort with modern technologies - it is highlighted. These board members then face challenges of a somewhat foreign technical vocabulary and/or appreciation of the technology terminology (Cerin, 2020). One of the interviewees, opined that,

"They (board directors) tend to be people who have previously been chief executives or CFOs who were, for example, sales and marketing driven. And so, there is a lot less technology experience there, and they're not digital natives, so they have spent the majority of their life in

an analog world… They're all for the most part, very skilled professionals in the career that they've had, and you've got to just make sure that you've got good balance of people with strong analytical skills, are capable of understanding cybersecurity risk and ask pertinent questions about how the organisation they are director of is addressing those cyber security risks." - Participant 28

Similarly, the other views also centred on the changes that governing boards are adapting to, with respect to composition and skill-set related characteristics. Another view pointed out that in recent years, having one or more board members with specific expertise in technology is also not uncommon; they are then able to have adequate conversations comfortably with the executive team (Landefeld et al., 2017) about technology in general and cybersecurity in particular. A participant explained this development in the following words,

"I think there's much more diversity of experience. We would never have brought in an IT person to sit on the board. We do now. Generally, having an experience of running large-scale transformation or IT or technical projects is a much more usual skill to bring into the board than it ever was before." - Participant 15

Generally, there seems to be a consensus that board members are increasingly cyber-aware, varying according to the needs of their respective organisation. It may be motivated by the willingness to protect the interests of one or more sets of stakeholders but the board's level of cyber awareness, including informed insight into cybersecurity risks (Cerin, 2020), has certainly improved within the last decade. One of the interviewees mirrored this view, by saying,

"I think I've seen boards certainly understand the implications of cyber security much more broadly and actually a bit more specifically in terms of understanding the risks and the technical risks… I've seen, in order to particularly safeguard the shareholders, a lot more effort being placed on understanding those risks, perhaps to where we were, probably five or maybe even sort of eight years ago. So, I've seen quite a change; a positive change in that respect." - Participant 27

In this way, the dynamics of board composition, its characteristics have also evolved with increasing digitalisation in the industry. Cumulatively these also impact the way the organisation decides its stance on cybersecurity. The next subsection explains the eventual decision-makers who are the ultimate leaders whose stance on cybersecurity would decide the organisational governance mechanism for cybersecurity as well.

4.3.2.2 Final decision makers for CS

As pointed out previously, the governing board and the chief executive together govern the cybersecurity strategy of the organisation. However, decision-making is far more nuanced than simply assigning it to one or the other. Especially for a technical area such as cybersecurity, the views have differed by organisation. The following section discusses such views.

One of the interviewees who interacted with large organisations as clients seemed to have a bird's-eye-view of the level of involvement of the organisations' boards in cybersecurity matters. According to them, it differed by industry and their dependence on technology. Outside of higher-risk retail and financial industries (financial crime is increasingly being committed in cyberspace (Nicholls et al., 2021)), boards may not even need to hire a director with specialist expertise (Landefeld et al., 2017). They said,

"...If it's a business that is highly dependent on its IT and that's a really big issue, they're likely to have someone more senior dealing with it. If they are a company that is less dependent on their IT and they perceive security to be of lesser risk, they have someone more junior on it. So, I think there's a full spectrum of having someone relatively junior in the IT department that does cyber security, as an addition to their day job, versus having some C-Suite members solely responsible for cyber security or security. And I think that's a manifestation of the companies and how they view cyber." - Participant 24

The same individual pointed out the day-to-day management led by the chief executive team, which had processes and people in place to manage the technology aspect of cybersecurity. Practitioner reports also cite evidence of security concerns being highlighted to the highest corporate levels translating to the necessary personnel being involved (Barnes, 2019) throughout the process. The interviewee further pointed out that unless a major cyber-breach had occurred, it was unlikely that the board would be involved. They opined,

"The board does not need to know each time we have a phishing email. They might need to know when we have a phishing email and we've been successfully compromised and that we're having a major incident... We might inform them. They probably only need to get involved in that in terms of actually issuing any direction if something really bad was going on with the operation of the business." - Participant 24

The above comment was an appropriate example of large organisations and their approach to cybersecurity. Research points out the critical role played by boards, management teams, and audit/risk committees (Landefeld et al., 2017) in mitigating security breaches (Hartmann and Carmenate, 2021). There, it is often managed by the chief executive team, with an expert in the form of Chief Information Security Officer (CISO) (Wessels et al., 2021), who communicates with the board. The CISO often has to shoulder the responsibility of explaining the cyber risk implications (Cerin, 2020), the consequent cybersecurity stance of the organisation, and accordingly requesting funding (or additional funding) from them. However, it is then the board's mandate to scrutinise and review the utilisation of the funds and the associated impact on the organisation's cyber threat landscape.

The above highlights the tandem between the board and the chief executive which, in cases where it is running smoothly, would be demonstrable through CISO requests being approved, thereby eradicating delays which could be especially challenging in fast-moving spaces like technology and cybersecurity. Studies are increasingly supporting this perspective, pointing out the crucial role played by the CISO, while the bulk of the responsibility lay with the Board and their executive team (Nolan et al., 2019). One of the board members was able to share a glimpse of the workings of the board-executive relationship on cybersecurity with the following words,

"I mean, you know that there's a given budget every year - you either manage this strategy within that budget, or you have to ask for extra capital. And then if there's extra investment needed, that's a board decision. After an increase in budget to be spent on something which hadn't been planned, you would do a review to see if we get what we said we were going to get with that money. So, you'd have a scrub up at the end to make sure that it worked, and it made a difference… It's (technology) more measurable than almost anything else that I know of." - Participant 15

Another participant was able to further explain the scrutinising role of the board in terms of making the best decisions and reviewing them for their organisation. They raised pertinent questions (Landefeld et al., 2017) that the board could ask the executive in their oversight role, arising out of their 'duty of oversight' (Landefeld, Mejia and Handy, 2015). Explaining these questions, they said,

"Let me give you an example. So, a question would be, 'When did we have our last penetration test? What was the result of that penetration test? What did it tell us? So, in terms of how we handle incidents, can you guarantee that we have an offline secure backup? When did we last exercise recovery from that backup? Have we table-topped the whole host of - how do we work with suppliers? What guarantee do we have that our suppliers are secure?' So, I think what the boards get from the executive is a clear sense of what we most need to protect – the number one issue. What do we really most care about? What are our cybersecurity weaknesses? And if they say there are no weaknesses, they're either lying or they're incompetent. And what is our plan for addressing those issues? And how do you prioritise the risks that come with it?"
- Participant 29

The above quotes from the participants demonstrate the immense responsibility faced by the decision-makers of an organisation's cybersecurity strategy. Creating a strategy that is operationally effective and efficient is teamwork and requires the experience and expertise of all involved. Together, these steps impact the way the organisation can defend itself in the cyber space.

4.3.3 Summary of Theme 1

The first theme focussed on the organisation as a collection of elements which together decide the degree of priority bestowed on cybersecurity, and the consequent stance on governing and managing it. Cybersecurity strategy-making and implementation are highly nuanced and layered processes which are subjective to each organisation. The combination of elements: its size, life-cycle stage, geography, industry sector, leadership mechanisms, governing boards, and their dynamics (to enumerate a few) determine the way cybersecurity may be prioritised by the organisation with respect to needs, which are then fulfilled by the organisational cybersecurity mechanisms. The next section explores the second theme which emerged from the primary research of this study.

4.4 Theme 2: Challenges to Robust CS

In the previous sections, we have observed the organisational features which impact the organisation's choice of stance on its cybersecurity governance. In the following section, we are going to closely look at the challenges which make cybersecurity management and governance a mammoth task. These challenges may be divided into two main sub-themes - one arising from cybersecurity incidents previously faced or those faced by peers, and the other from a range of unforeseen challenges. These are discussed below.

4.4.1 CS Incidents

Cybersecurity incidents are some of the biggest challenges that organisations face on their path to creating and executing their cybersecurity governance mechanisms. Many participants pointed out that each day, a large organisation faced hundreds or more cyber breach attempts. However, their existing cybersecurity measures ensured that these attempts were not successful in compromising the organisational cyber assets. In recent years, with circumstances exacerbated by global events, these instances of cyber breaches have risen exponentially. The aftermath of these incidents has been a range of losses, sometimes limited to financial and/or legal in nature, and at other times leading to the termination of the small or medium-sized enterprise (Abraham and Sims, 2021).

Many smaller organisations, or those which are not prioritising cybersecurity, and sometimes even those who are, are unfortunately successfully breached by threat actors. The damage to larger organisations is multi-faceted - reputational and financial loss, legal actions by victims, and loss of customer trust (an indirect risk (Wessels et al., 2021) and at times more severe than legal/ financial loss (Nolan et al., 2019)) - and immediate in their impact. However, the damage from cyber incidents varies, and may be considered unique in each instance. The damage was explained by one of the participants, as following,

"… Because of a cyber-attack or because of something like that, the sufferage (damage) is not only in terms of losing customer trust but is also revenue related. Something goes down for a few days or even few hours and the amount of revenue that a company could lose could also be massive." - Participant 22

The attack itself may be intended to have varied impacts, which would then influence the duration and intensity experienced by the organisation which underwent the attack. Literature has underscored the impact risk has on reputation and, further, the role played by reputation in mitigating risky events (Kewell, 2007), which emphasises the risk of cyber incidents and their potential for organisational damage. Scholars have found that amongst the many losses from cyber-attacks, financial losses occurring due to the work stoppages, rather than loss of data itself (Nolan et al., 2019) were perhaps the most significant. Another interviewee explained that the types of these damages would vary depending on the type of attack perpetrated by the cyber-criminal by giving examples, saying, *"So, there are different ways that cyber-attacks can affect an organisation. So, there's espionage - where somebody like a state-sponsored actor might be trying to steal informational secrets from the organisation. There is an availability question wherein the organisation provides a service, and it can be knocked offline by a cyberattack like a ransomware attack. There is a data destruction aspect - here you worry about the data being destroyed or getting leaked into an area where it becomes risk from a GDPR perspective. You've got intellectual property theft as well. And then, on top of that, you've got just general financial loss. And you've got reputational risk as well."* - Participant 25

While there may be different kinds of attacks on cyber realms, the damages could be from sources previously not considered, such as from legal expenses and regulatory penalties. These were described by another interviewee who hinted at the regulatory (Landefeld et al., 2017) and financial aspects of criminal attacks, when the organisation is required to pay the fines levied by the regulatory authorities, which in itself may pose a considerable additional financial burden on the already impacted organisation. They said,

"Because our customers really do value our service, a loss of reputation is really something that we would find really painful. Um... directors being taken to court? Yeah, maybe not massively worried about that 'cause we do the right things. A lot of the time (there are) dumb penalties from regulators. Now that is one that should worry everybody. So, we're talking about a heavy fine from the ICO (Information Commissioner's Office)." - Participant 21

However, recent years of cyber incidents have worked miraculously in garnering growing focus on this field from organisational rivals and peers (Ashraf, 2022), who want to avoid similar damage. In cases where the damage can be pre-empted, it is even supported by academic research in the realm, supporting the preparedness to cyber breaches as a mechanism that may be relied upon. This preparation through routines may be recognised as a valuable dynamic capability (Eisenhardt and Martin, 2000; Zollo and Winter, 2002), and the fortified security itself is a precious resource (Barney, 1995; Barney and Clark, 2007a) to the organisation, with potential for future opportunities. Sallos et al., (2019) pointed out that if the occurrence and consequences of the breach can be understood in advance, then the organisation may be able to adapt to the breach's destructive potential.

"And when somebody else gets breached, you know that whilst we have that empathy for our peers, we also need to take advantage. And a breach that somebody else suffers is almost gold

dust because it gives you an opportunity to look into your systems and the people you're working with and see what they're doing. And if you find you're using the same and you're vulnerable, very quickly the investment comes forward because your organisation, or the organisation you're working for, doesn't want to be the next headline, so that makes a difference." - Participant 8

Understandably in the course of running the business, any incident - big or small - would lead to damages but, very often, an organisation is forced to re-evaluate its cyber mechanisms and measures (Wessels et al., 2021), overall cybersecurity stance, and its robustness in preventing future attacks. In organisations where cybersecurity is not on the standard board agenda, a cyber incident triggers a substantial nudge in promoting cybersecurity conversations at a board level, which has been mirrored in studies (Gale et al., 2022). Literature has supported the view that small failures (in this case, minor cyber incidents) contribute to effective learning (Sitkin, 1992), offering unique insights, and allowing valuable lessons to be learnt from minor cyber incidents while on the path to robust organisational cybersecurity. Another participant mirrored these sentiments citing infamous incidents as learning, saying,

"I mean, obviously there's lots of lessons we can learn… from everything from the Maersk compromise all the way through to WannaCry in the NHS." - Participant 27

One of the biggest learnings that seemed to emerge from organisations which either survived cyber incidents or learnt from observing their peers (Ashraf, 2022) was the inevitability of cyber incidents (Ablon and Libicki, 2015). Scholars have highlighted the seeming inevitability of cybercrime within the cyber realm as the potential of having *barbarians always at the gate* (Trautman, 2014). Microsoft, as a leader in the technology industry, is recognized to hold it as one of its mottos, lending credit to the notion of '*when* and not *if* an organisation is breached' (interviewee 16). It attests to the increasing acceptance of this truth among experts to imagine that a breach is bound to occur sooner or later (Ablon and Libicki, 2015). One of the interviewees articulated it by saying,

"When SolarWinds and FireEye, some of these enormous companies who themselves… their whole product range is to prevent data loss for clients… and then they get breached, it just demonstrates that nobody is immune. And it demonstrates that all of the basic controls are just so important." - Participant 8

Understandably, cyber incidents lead to considerable impact on the reputational (De Minville, 2020; Gale et al., 2022; Nolan et al., 2019), financial, legal, and functional aspects of organisations. But their growing numbers and list of famous victims do testify to the significant probability of breaches in every organisation. Many organisations which survive them are rendered nonfunctional for extended periods of time, thus making cyber incidents one of the most significant challenges against maintaining and implementing a robust cybersecurity practice. It may then be surmised that cyber-attacks thus hold the potential to cause irreparable damage to an organisation. At the very least, these alter the course of the organisational path from that of progress and evolution, to one marred by crisis in its management.

4.4.2 Macro-economic Challenges

Moving beyond the cyber breaches, there are varied kinds of other challenges that organisations face on their path to crafting a successful cybersecurity governance system. Many of these challenges are beyond the control of the organisation. However, the more these are observed and learnt from, the easier it is to adapt to them and make necessary changes to affect a successful cybersecurity policy and practice.

4.4.2.1 Pandemic

The Covid-19 pandemic has proved to be one of the biggest contemporary challenges faced in recent times. It brought, not only individuals and organisations, but also entire economies to a veritable standstill. It was a milestone event, especially for the cybersecurity industry, as it exposed the underlying vulnerabilities in the way businesses were carried out by most firms. The pandemic was also exploited by several threat actors where, besides the business's inability to function, the challenge was exacerbated by their virtual assets laid bare through breaches and attacks (Hubbard et al., 2021).

Natural events have the potential to significantly impact communications and IT infrastructure (Boyes, 2015), thereby adversely impacting an organisation's cyber realm. One of the participants alluded to the increased risks and vulnerabilities being faced by organisations, owing to the pandemic, with the following reasoning,

"So, I think there's all sorts of risks that have come into it (with pandemic). I think what's happening is that probably the reason the risk increased is because it's been such a fundamental change. The way people work, all of the risk assessments done before Covid… to pick up all of the things that changed… I can see that just the fundamental changing of people's

working procedures must create risk because the risk assessments were done pre-Covid. There are things that change that nobody was spotting." - Participant 11

Another interviewee working as a virtual CISO (externally hired consultant (Landefeld, Mejia and Handy, 2015; Landefeld et al., 2017) working as a Chief Information Security Officer) to a large organisation, was able to summarise the extent of risk with two startling figures, while adding that the increase in resources diverted to cybersecurity measures was not commensurate with the rise in risk.

"… The risk has increased… I mean we see reports of phishing attacks have gone up by 300%. I've seen that ransomware attacks have also gone up significantly with a similar kind of percentage. Anywhere from 150 to 400%... I've seen being quoted on all sorts of graphs and charts, as you can imagine. So yes, the threat has no doubt been greater, but it doesn't necessarily mean people are prepared to spend that money." - Participant 8

Whether the pandemic has exacerbated the organisational vulnerabilities may be open to debate; however, it has certainly exposed the cyber vulnerabilities, which are exploited by cyber criminals. Increase in hybrid working options like working-from-home (WFH) have facilitated cyber-attacks like phishing, scams through less secure internet networks (Pranggono and Arabo, 2021). One of the interviewees explained the way in which the risks presented themselves as a challenge during the pandemic, offering a great insight into pandemic-induced challenges, saying,

"I think the challenge is if you consider before the pandemic, maybe 20% of people worked at home for one day a week, on a Friday. But there was a process in place. What you had to do was scale that process up, to go from 20% of the people one day a week to 100% of people five days a week. So, the checks and balances in place have to be able to cope with that many more people. And then also I just think the flow of data is safer within the same building, (with the remote working) it is all over the place. The data is just flying… there's a lot more points where someone can potentially capture the data." - Participant 11

In this way, the pandemic has perhaps irrevocably changed the entire paradigm of business function (Pranggono and Arabo, 2021), with options of work-from-home/hybrid working brought permanently to the fore. In certain ways, the degree of reliance on the digital realm is considerable. This may be considered the time of unprecedented convergence of physical and cybersecurity (Wirth, 2020). The scale of remote work, the lack of control of potentially unsafe data networks, and less overall secure systems and locations have added multi-fold challenges to an already sensitive cybersecurity management system.

4.4.2.2 Industry-level challenges

In this section we observe more challenges that businesses grapple with on their path to securing their cyber realms. These challenges could broadly be categorised in four sub-sections. These four relate to the human capital/resources aspect of this industry (which is highly specific and technical), the dynamic nature of technology (and its constant evolution impacting cybersecurity systems), the resources at the disposal of criminal actors, and the often-overwhelming range of options from which to choose the best cybersecurity services/products.

4.4.2.2.1 People challenge

The first of these challenges starts at the very beginning of concerns, which looks at the aspect of human resources in this highly technical field. Understandably, as this area is fairly recent in its development, it is inconceivable to find experts with decades of experience behind them. While people with adequate experience often have their pick of positions to choose work from, they are consequently disproportionately expensive to hire. Furthermore, hiring adequately qualified experts is a challenge unto itself; the ability to hire an expert of the field also requires adequate experience of (or familiarity with) the field. This is also exacerbated by the fact that highly skilled tech experts may also prefer to work with organisations or sectors, where they are assured of being appreciated and not having to expend a portion of their efforts convincing the boards of their need.

Many of the participants agreed on, highlighting that, first and foremost, most cyber incidents occur as a result of errors made by human (Thackray et al., 2016) beings handling technology. Technology is handled by humans and people make mistakes (Mulligan and Schneider, 2011) - this is the accepted summarisation of this aspect of the people-challenge. To delve into the reason behind this would reveal that many of these instances are crafted in such a way by threat actors so as to attack the human vulnerability of this technology-based field, which are termed as ‘social engineering attacks’ (Conteh and Schmick, 2016). Perhaps it then is necessary that not only are the employees (the people who are the vulnerable access points) trained, but the policies and procedures (Wright, 2021) involving them are also strengthened. The interviewees thus urged on processes to train the humans managing technology better, saying, *"I'm a firm believer that if you have 100% attack vector, 90% of the initial compromises (are) because of people making mistakes, (so) invest more in the people, so they make less mistakes."* - Participant 14

In the digital age, with the current cyber threat landscape being volatile and increasingly complex, scholars have observed that cyber resilience (World Economic Forum and Accenture, 2023) is an important component of a robust cybersecurity stance. Furthermore, to fully realise the potential of cyber-resilience, organisations are being called upon to implement a comprehensive approach to cyber-resilience, which would incorporate enterprise-wide cyber-awareness and implementation (Abraham and Sims, 2021). This highlights the necessity to hire, train, and retain personnel who are able to protect an organisation's cyber-assets. Furthermore, another participant mirrored these sentiments highlighting the vulnerability posed by the fingers operating the keyboard, saying,

"Yeah, so many of them now are socially engineered. You know it's very rare that something gets through purely of its own volition, because it's just such a powerful piece of code or brilliantly written malware that you know somebody somewhere has to do something stupid - a human has to make a stupid decision for these things to work." - Participant 28

For organisations choosing to hire these professionals, specific skills in the arena become the focus. For instance, information security, computer systems, and computer administration (Bana et al., 2022) are popular skills related to cybersecurity. However, for firms having experienced data breaches, the demand for skills even pertaining to public relations and legal talents are found to be on the rise. Thus, the overall concern is hiring individuals with the requisite skills, as necessitated by the organisation. A different interviewee mentioned the skills gap as a considerable challenge for them, which contemporary studies are increasingly illustrating (Nodeland et al., 2019), with the following,

"So, it's a big cliché, but the skills gap is a real issue for us at the moment… and it's often very difficult to place people because they might have only a few years of experience, but they might be really high calibre… and that could be great. Or it could be that they think they're worth a huge amount, and so we have a bit of a gap in terms of - 'is this person worth the salary they're asking?' And then at top level, we have the leadership roles, so we need those as well." - Participant 23

Another view that the hiring challenge brings to fore is the observation that a cyber-breach event triggers firms into hiring cybersecurity professionals (Bana et al., 2022), but prior to such events, this may or may not be a firm priority. It is even less so if the organisation is within the public sector (and under-funded, thus under-prioritising cybersecurity) and/or facing minimal media coverage of such negative events (and not feeling external pressure to need such personnel).

Another important aspect of the people challenge within the cybersecurity stream was voiced by an interviewee, putting the difficulties in hiring of cybersecurity personnel into focus. Literature would support this view of the importance of human capital as a significant resource to the organisation (Bana et al., 2022; Barney and Clark, 2007a, 2007b; Wright, 2021). One of the interviewees explained the challenge from a hiring perspective, saying,

"How do you judge the quality of an individual doing a job when you've never done it yourself? In a technology-based company, arguably, people that enjoy technology and are good at cybersecurity, have a certain mindset… a certain approach and they might deviate more to that type of organisation because they hold the same sort of values. Whether you want to be the first of an IT person to join a retail company, for instance, you may well be a lone voice, and it may be much more challenging." - Participant 13

These instances cover the wide variety of challenges within the human capital aspect of cybersecurity challenges that organisations often face on the path to fortifying their cybersecurity governance mechanisms.

4.4.2.2.2 Tech acceleration challenge

Even when an organisation is successful in hiring and retaining its cybersecurity experts, they subsequently face the challenge of keeping up with the fast-paced evolution cycle of technology itself. Research underscores the view that technology changes rapidly, rendering recent dominant technologies obsolete (Kosutic and Pigni, 2020). Unlike a few other strategies, technology does not come with a long shelf-life, which would render a periodic policy (such as an annual policy) inadequate. It expires quickly, and such dates are difficult to forecast in advance, while their perishability is the only constant. This complicates the challenge of maintaining robust cybersecurity, as creating one policy for one time period, for instance, would be inadequate.

"The market is changing… technology is changing, right? And you're constantly struggling with how to get your team to move at the same pace with which the market and the technology landscape is changing. Because the technology world is actually going through a massive acceleration and it's almost humanly impossible for 95% of your workforce to keep in step. So, the problem then for leaders like us is, how do you drive these people to start thinking about what the technology industry demand (is) today versus what it demanded five years back?" - Participant 2

Furthermore, technology evolution also leads to evolution in criminal methods (Bejan, 2022). The insight from this thought was further elaborated on by another participant who used an analogy to explain the inadequacy of popular cyber certifications, which organisations largely rely on to demonstrate their cyber compliance. Even research reflects this view, stating the inadequacy of current certifications, urging the need to automate the risk assessment and testing processes, to enhance the framework success (Matheu et al., 2021). They said,

"There's no guarantee… even an organisation that is certified - let's say an ISO 27001 or NIST or SOC2, PCI DSS - all of these things can be externally audited and certified. They are only a point-in-time status review, really. I compare it to an MOT on a car. At that point in time, they were certified as being compliant, and that means they had all of the controls in place and maintained the particular controls (that) the framework required. However, they need to maintain that going forward. Just because you have an MOT, doesn't mean the brakes aren't going to fail on you three months down the line, that type of thing, and you're gonna have an accident." - Participant 8

Yet another concern related to the technology acceleration aspect of the cybersecurity industry is especially faced by smaller organisations or those in the public sector, as supported by studies presented in practitioners' journals (Hubbard et al., 2021). As these organisations, in particular, suffer from a lack of adequate funding, they often rely on legacy systems which are extremely challenging (if not impossible) to modernise, and also introduce cybersecurity issues (Axelrod, 2015) associated with cyber vulnerabilities magnified and exposed to a potential threat actor. A participant was observant of this insight, when they pointed out,

"Well, legacy is a problem because the older the system, then probably it's highly likely that they are more vulnerable." - Participant 31

Cumulatively these challenges also add another layer of complexity to the puzzling cybersecurity governance matrix, rendering the work of ensuring robust cybersecurity mechanisms even more complicated. In the next subsection, we examine the challenges caused by the virtually indefatigable nature of cyber threat actors.

4.4.2.2.3 Criminal motivation/access challenge

Criminal minds hoping to breach organisations come in a wide variety (Rai and Mandoria, 2019), ranging from solo individuals with a latent talent in breaching (for the sheer pride of being able to cause a cyber breach) to others sponsored by states/governments (Brantly, 2014) intended to cause financial disruption or even wars. Very often, these threat actors have the access to extensive resources as well as the motivation (Chng et al., 2022) to perpetrate all kinds of cyber-attacks. We explore some of these here.

One of the participants noted that the motivations of these criminals (Rai and Mandoria, 2019; Thackray et al., 2016) was substantial on account of the volume of financial gains to be experienced from breaching large organisations. While literature supports this idea, it also brings forward other reasons such as recreation, prestige, revenge, and ideology (Thackray et al., 2016), within criminal motivation in the cyber realm. They said,

“There's so much money to be made out of hacking/ fraud, whatever you want to call it. You're only ever one step ahead or one step behind, which is why you have to stay on top of it. You can never be certain… you have to be constantly looking to see what's going on.” - Participant 10

Some other participants reasoned that besides the financial motives (financial cybercrime - primarily for economic gain - being increasingly conducted in cyberspace (Nicholls et al., 2021)), there is also the attraction of customer data (Michael et al., 2019) which makes cyber breaches more challenging to prevent for organisations, and more attractive for hackers to instigate. One of the interviewees highlighted the type of organisations susceptible to such threat actors, saying,

“If you're a health insurer or a life insurer or motor insurer, you carry a lot of personal information about individuals. You've got names, addresses, dates of birth, health records, criminal convictions. Maybe (even) credit card numbers. That's the kind of stuff that these hackers and their companies love.” - Participant 20

A different participant was more pragmatic about the field of cybersecurity emphasising the imbalance between the resources and motivation of the organisation attempting to protect its cyber assets, and those of the cyber criminals seeking to violate them. They pointed out,

"You will never be able to outrun the bad actors ever… that is the nature of cyber security. You will do it in a point of time and then because of the nature of their business, they will change and adapt to overcome the control or the mitigation, if they're really that interested. If you're clever about it, you can spend much less effort, time, money, and investment resources around it, but ultimately the threat actor is always going to evolve and you're never going to be able to stop that." - Participant 27

With an increasing number of motivations, classifications of the criminal and their potential to harm, and the kinds of strategies employed by them (Chng et al., 2022; Rai and Mandoria, 2019), the world of securing the cyber realm is becoming increasingly complicated. On the other hand, the world of cybercrime is incredibly lucrative, often supported by the wide-ranging and complex market structure available for this type of crime. This market is equipped with the latest technologies, constantly growing, maturing, innovating, challenging to shut down, and easy to enter by cyber-criminals (Ablon and Libicki, 2015). Understandably, this market then acts as a support system for cyber-criminals, both new and old. Pointing to the vast array of resources that cyber threat actors have access to; another interviewee emphasized the relative ease with which cyber criminals can breach organisational cyber realms without even being technical/cyber-experts themselves. They said,

"There are lots of organisations who are creating software out there that you or I can buy off the shelf, and create a ransomware attack ourselves. It's just so much easier… you don't even have to be a technical wizard to attack nowadays. You don't have to have people who are out-and-out hackers… you can buy the software which has a full support package – Ransomware-As-A-Service. So, these developments are quite worrying." - Participant 8

All these together make the field of cybersecurity even more challenging, owing to the high stakes- high motivation (Chng et al., 2022) from the perpetrators of cyber incidents. With the evolving digital landscape, criminal intent is also developing into a progressively complicated genre, thus making cybersecurity an increasingly arduous task. Organisations, thus, progressively are perplexed by finding adequate means to fortify their cyber realms in their present and future.

4.4.2.2.4 Big market for CS products challenge

Protecting the cyber realm of an organisation is often made further challenging by the enormous variety of cyber solutions available in the market. From amongst these, finding the appropriate fit for one's organisation, ensuring that it stands the test of time, and be able to replicate the process over time, increases the complexity of ensuring robust cybersecurity. Ironically, the availability of several alternative solutions (Wessels et al., 2021) poses a challenge to implement the mechanism most appropriate for each organisation.

This subsection throws light on challenges of this nature. As previously highlighted in 2.2.2.3, the cybercrime market is incredibly complex and attractive. Research confirms that such a market includes an entire network of suppliers, potential buyers, vendors, and intermediaries working together to facilitate cyber based crime. It has even been compared to and found more attractive than drug trade, with respect to the ease of entry and the economic output to be gained from it (Ablon and Libicki, 2015). One of the interviewees expressed their incredulity of the massive cybersecurity solutions market, explaining in these words,

"There are endpoint security products, there are network security products, and then there is managed security. So, from the solutions perspective, I think the market must be around 150 billion plus. It is a massive market, and a big organisation can actually have almost like 50, 60, 70 different security products - all doing different things. So, we say cybersecurity, but it's a very broad market." - Participant 22

Another participant highlighted that the variability of interpretation of different individuals within the same organisation also adds to the complexity of choosing the most appropriate cybersecurity solution for one's organisation. They said,

"What are we talking about when we say cybersecurity? What do we mean by that? Because you can get like 50 different definitions of what cybersecurity means according to any particular book, so now it doesn't really matter that there are 50 different ways people could describe it. What matters is how do you describe it in your organisation, and does everybody have that same understanding, so that when you use those words, they have the same meaning to everybody. Because otherwise, you're just constantly talking at cross purposes." - Participant 28

Finally, the astounding range of options available within the umbrella term of cybersecurity is not merely perplexing for an average professional. Subject experts and seasoned professionals with relevant experience in cybersecurity are also challenged by this aspect of the industry. A participant raised some elementary questions which could befuddle even seasoned experts like CISOs, saying,

"It's overwhelming. You know, even as a CISO who understands the market, it's still quite overwhelming. Which technology provider should I go with? Which platform protection level should I go with? Oh, do I need the bronze or silver or the gold? And of course, it's turned into a bit of a sort of snake oil business." - Participant 27

Such complications available as humongous options of cybersecurity solutions further add to the challenges faced by organisations in safeguarding their cyber assets. In the next section, we explore a few ways which have emerged from the data as effective tools to tackle these challenges.

4.4.3 Summary of Theme 2

Theme 2 proceeds a step further from theme 1, which focussed on organisational needs, by presenting the array of challenges complicating the task of securing organisational cyber assets and realms. All organisations - large or small, technologically evolved or otherwise - are presented with various challenges which are unexpected, sometimes unprecedented, and understandably improbable to prepare for. Yet, in a dynamic and ever-evolving technical field, adaptability and alertness are non-negotiable traits for an organisation to rely on. Similar to any other challenge a business must encounter, even cybersecurity-related challenges can hope for adequate implements to overcome them. The next theme and section examine these tools which are invaluable on the path to fortifying organisational cyber realms.

4.5 Theme 3: Tools for Confronting CS Challenges

In the previous section, we explored the variety of challenges which complicate the search for and efforts to fortify an organisation's cyber realm. In this section, we now discover three primary implements with which to confront these challenges. These are described below.

4.5.1 Board Engagement Levers

This subsection highlights those levers which have the potential to promote board engagement which consequently enables the organisation to award cybersecurity the adequate attention it richly deserves. These centre around the board's ability to appreciate the risks and costs associated with poor cybersecurity mechanisms as well as the inhibitions board members suffer from having limited prior experience or exposure to cybersecurity.

4.5.1.1 Risk associated with CS

Cybersecurity risks are increasingly on the rise within organisations, irrespective of whether they are being perceived for discussion. Even in cases where the junior staff/IT teams are actively involved in reducing these risks, as we have observed through previous sections, unless the leadership gets involved, the organisational stance does not change. Thus, the involvement of governing boards in these discussions will amount to their appreciation of the risks (Cerin, 2020) emanating from poor cybersecurity measures. One of the interviewees emphasised the significance of keeping cybersecurity risk related discussions a continuing agenda by saying,

"You often see there will be like a regular sort of report - whether it's monthly or quarterly or annually - from your technology team, whether it's an IT operations team or as a separate sort of a cyber-focussed team… but something that explains to the board what they're doing. But those conversations around risks and changes to risks and the cyber element of risk should be as continuous as they need to be, depending on what you're doing as a business rather than just once a year. Because cyber is an increasingly big part of that risk profile for a lot of businesses, I think." - Participant 28

Research indicates an encouraging trend wherein governing boards are able to appreciate the risk presented from cyber sources, prioritising it as a macroeconomic risk deserving of priority (Nolan et al., 2019). However, this is not always the case. A participant astutely observed that, in a considerable number of cases, the boards are not familiar with the risks they face, inhibiting adequate action or timely intervention. According to them, if boards were able to surmount this obstacle, they would seek help and answers, even if that came from technical and/or cyber experts. They pointed out,

"I do think that having expertise in cyber security and a number of other key areas is vital, as much as anything to mitigate risk. And I think boards themselves are not so good at understanding their own risks, what they are, how big a risk that might be, and the impact that might have. I think if they understand that, they will then get the expertise to mitigate whatever those risks are because they understand that they don't have the expertise in-house… and then they will obviously get those individuals to join to hopefully help mitigate some of that effect." - Participant 13

Furthermore, upon recognising the inextricable links between risks from crisis events (such as cyber-incidents) and organisational reputation (Kewell, 2007), some useful insights were gleaned from the data collection. One participant was forthcoming on the kind of conversations which are needed to help the board appreciate the cyber risks involved in doing business, so that the cyber strategy is robust. Their thoughts involved a hypothetical conversation between them and the board, saying,

"You know, you don't go to your board and talk about SQL injection vulnerability in your website? That's not the level of conversation you have with those people. What you talk about is, 'Oh guys, you remember that risk of our customer data walking out of the business, and the fines that we could get, and the reputational damage that we could suffer as a consequence?' And they'll remember that because we had that conversation as part of the strategy, and they'll go, 'Yeah, (name), what's the problem?' And I'll go, 'Well, there's a risk and we need to fix that.' and they'll go, 'Tell us what we need to do.' And that's the dynamic." - Participant 21

For boards to better appreciate the risks (Landefeld, Mejia and Handy, 2015) involved in organisational cyber defence mechanisms, it is also vital to understand where the risks culminate from and how they vary across organisations. This understanding would ordinarily involve exploring the cyber threat landscape and the cyber intelligence that the mechanisms collect for the organisation. Preparing a plan specific to the threats and implementing (Barnes, 2019) it would largely prevent a catastrophe. This was explained by another participant, highlighting the significance of identifying the most important assets - 'crown jewels' - (Hubbard et al., 2021) and then protecting them, saying,

"So, when you look at what the cyber threat is, most of it is derived from a clear understanding of what the crown jewel or the unique selling product (that your company offers) is, and its particular place in a global supply chain. All of those things play into a keen understanding of what the cyber risk is… and then the cyber threat intelligence program essentially uses that information to formulate a collection plan of what are the things that we're going to pay attention to, what are the things that we need to know, to protect ourselves. So, it's very much a forward-looking posture, based on (the) understanding of risk." - Participant 19

Taking the conversation further, another perspective which surfaced was the element of future wars which would invariably involve a substantial cyber component. A substantial number of conflict events in contemporary times is being sponsored by nation states, and increasingly the chosen platform is cyberspace. The specific benefit of cyber conflict to such state actors is the ability to influence the dominant space between overt diplomacy and overt war (Brantly, 2014).

Hence, strategically planning ahead to incorporate cyber as an elementary part of the product/service would be critical and valuable as an intangible resource (Hall, 1993) to the organisation, which would need to be appreciated by the boards. This was articulated by a participant, saying,

"Taking the (company name) as a defence contractor angle, for example, we build warships and planes, and then you know all defence equipment now. Cyber battle space is the 5th domain. So, going forward, wars are not going to be fought with the traditional means of land, sea, and air. Cyber is going to be a very important component. Which also means that whatever we are producing also has to be very stealthy, from cybersecurity perspective." - Participant 22

From the above comments it is increasingly clear that discussing cyber risks often, having the appropriate conversations and understanding the mechanisms involved in detecting threats are all vital towards warding off cyber risks. The next subsection outlines the costs associated with cybersecurity and the ideal perspective towards them, which allows governing boards to engage with the subject and take positive steps in it.

4.5.1.2 Costs associated with CS

Traditionally, technology has been associated with expenditure; however, relating cybersecurity to investments is still fairly recent and, unfortunately, not all organisations and their boards have reached that degree of realisation. A substantial number of organisations consider cybersecurity as a cost centre (which may be a consequence of their inability to appreciate the associated risks and implications) and hence, the budget allocations still leave much to be desired. One of the interviewees pointed out,

"Let's say if it costs you a million and you know that (with) the kind of nature of my business, I will have to invest like 5,000,000 to get it all secured. Then at the board level, I think that's also a conversation to have - you don't see the benefit of that investment. And you don't see the returns of it or the advantage of doing more. So, I think the harsh reality of it is, it's (cybersecurity) still seen as a cost centre. A business, unless it's related very nicely with the competitive advantage and improving the customer trust, a lot of businesses still take it as this is something they have to do as a checkbox exercise." - Participant 22

During the interviews, it was commonly noted that organisations could generally be considered myopic with respect to allocating resources for cybersecurity measures unless they had instances to learn from, which may have affected their behaviour. Literature also finds that a lack of adequate ROI (return on investment) (Barnes, 2019) may inhibit appropriate spending on cybersecurity measures, even though certain research bolsters the link between IT spending and beneficial return on investment (Aldasoro et al., 2022). Furthermore, some scholars have illustrated a relationship between cybersecurity expenditures and the potential damage from cyber incidents through a Gordon and Loeb model (Krutilla et al., 2021); yet the practice is not commonplace. One participant highlighted the inability of the boards to see a linear relationship between the cybersecurity investments and the return they received as a result of it. They said,

"I think what's interesting is a lot of companies that are kind of unwilling to make that investment because you don't invest £5 in there for £10. So, it's a bit more intangible: you invest £5, and over the next 10 years you'll probably get £20 back, but you don't see the direct link between investment and return on investment, so it's a lot harder to prove the value of it. And companies… they've got profit motives and they've got budget restraints… all the usual stuff. And it's something that I think a lot of companies are maybe less so now, but certainly some years ago were not willing to really spend money on because it was seen as a bit of a dead cost." - Participant 20

It may be reasonable to imagine that in a global pandemic, when the cyber risks faced by average organisations rose exponentially, the organisations would have risen to the challenge and started allocating more budgets for tackling them. However, as one participant pointed out, it, unfortunately, was not the case. They said,

"So yes, the threat has never been greater, but it doesn't necessarily mean people have been prepared to spend that money. A lot of organisations, particularly the ones I was focussing on, were reducing their budgets for the type of thing I do. But I think I see glimmers of hope as we are starting to get out of this global pandemic. People are becoming a little bit more comfortable to invest, and they realise that things that they might have put off - regards security and data privacy - whilst they survived over the last nine months or whatever it's been, that they're going to have to tackle them again." - Participant 8

Another insightful perspective underscored the path to identifying the organisational investments necessitated by cybersecurity – through the assignment of a business value to the cost of potential loss as an outcome of unmitigated cyber risk. Research is increasingly highlighting the need for governing boards to assign adequate urgency to cybersecurity, associating it with the costs of financial damage of business disruption as a consequence of cyber breach (Nolan et al., 2019). One interviewee suggested comparing the costs incurred in bringing back normal functioning from a cyber-incident to the costs of ensuring robust cybersecurity, as a guide to deciding cybersecurity expenditure. They said,

"At the end of the day, compare that (cybersecurity expenditure) to how much it costs to get things sorted out. I mean, it's quite a substantial number. So, we're probably going to spend £2-3 million just to get things back in order. I would much prefer spending money on getting new machines for food production and getting things running more efficiently. But I understand if we don't have that, we are in big trouble… so it does make sense." - Participant 26

Another participant presented a more encouraging take on the change in behaviour, as is observed increasingly in organisations. According to them, the perception of cybersecurity expenditure is moving more from a purely financial decision to ensuring observance of compliance. Hence, it may be considered that it is receiving adequate focus. Academic research supports this view by pointing out that since there is a financial risk associated with cyber which is measured in monetary terms, organisations ought to observe it as part of their governance function (Nolan et al., 2019), which is encouraging. The participant articulated their view in the following words,

"Businesses, where data leaks could cause reputational issues, took it seriously… so the drive was more balance sheet driven. Commercial organisations always are driven by commerce because it needs to make commercial sense for them to do something. And GDPR, in Europe at least, completely changed everything because it became a personal liability for independent directors. So, it moved from a commercial position on the CFO's mind to a risk and compliance position within the company, where a certain budget was actually allocated for the purposes of cyber. And therefore, the IT gained prominence because of protection, risk gained prominence because of compliance, and the CFO allocated the budget appropriately." - Participant 3

The above comments explain the journey of realisation associated with cybersecurity costs that governing boards are becoming increasingly conscious of. While it may have traditionally been largely considered an economic cost (Wessels et al., 2021), it is now progressively being perceived as an investment - sometimes owing to its compliance association, and at other times due to its capability in preventing costs associated with incidents. These are all encouraging steps in the field, as it allows boards to closely engage with the subject and lead the organisation towards a safer cyber-future. The next subsection focusses on board members' inhibitions associated with cybersecurity, which have progressively been reducing in recent years.

4.5.1.3 Inhibition around CS

Cybersecurity, as we discussed in the sections 1.1.1 and 1.2.1, is often perceived as a technology-centred domain. Coupling it with the average age of board directors, cybersecurity has suffered from a lack of adequate conversations on it in the boardroom. For board members to unreservedly discuss it and make the necessary expenditure on it, the inhibitions surrounding this seemingly technology-driven topic need to be lowered. This subsection discusses the views of the participants bringing these thoughts to the surface.

The reality of having board members experienced in scrutinising decisions and the debate over the leadership teams' operational choices related to non-technical matters, makes it challenging to discuss cybersecurity - this is a learning from the practitioner's experiences. One of the interviewees articulated their thoughts, saying,

"Cybersecurity is one of those areas that lots of boards don't have experience in, and lots of directors don't have experience of. And I think sometimes that can lead to them maybe being a little more shy, I suppose, to ask questions 'cause they're stepping outside their comfort zone. Whereas, discussing a balance sheet and probing into litigation or whatever it might be, it's very comfortable for them and they know what questions to ask, 'cause they've been there, seen it, done it before." - Participant 13

The solution to the challenge in the above comment came from the thoughts and experiences of another participant. According to them, the key is to develop a comfort in asking questions which are outside of the ordinary comfort zone, even at the cost of being uncomfortable. This also supports literature which urges boards to have members who are comfortable asking such questions (Landefeld et al., 2017), and may additionally be considered a useful and intangible resource (Hall, 1993) facilitating board engagement in cybersecurity, for the organisation to draw upon in the course of business. The interviewee elaborated by,

"As a director that's one of the areas that I've seen, in the sense that I'm not an IT expert… so you know if the IT guy comes along and tells you this stuff, you kinda have to take them at face value. You rely on their answer. But the job is to challenge what I think and maybe ask the stupid question, in the sense that,' I'm not an expert, so I'm gonna ask you a silly question' to

see what the answer is. Because you just need to have that inquiring mind, I guess." - Participant 20

An important reason for board members to embrace the discomfort of asking seemingly silly questions arises out of the otherwise lack of conversation that the vital topic of cybersecurity may then be able to muster. In several cases, even the leadership executive, in charge of operationalising cybersecurity, is apprehensive of broaching relevant conversations for fear of inconveniencing the board (Landefeld et al., 2017), or worse still, inadequate understanding and support in the boardroom. This thought was highlighted by a participant, saying,

"Sometimes they make their way to the board, depending on how interested the board is. And also, as much as anything, how interested the executives - the CEO, CFO, and other executives (that are executive directors), how important they think the board will feel this is. Because sometimes there's a bit of a perception that we'll give them information, and they're going to say, 'Thanks very much.' If they're going to see it as a waste of 5-10 minutes, half hour/an hour of their time, then we're not going to put it on the agenda 'cause we don't wanna look silly." - Participant 13

In either scenario, the inability of the boards to appreciate the discussions around cybersecurity creates an obstacle to taking adequate steps towards robust cybersecurity mechanisms. In several cases, the board members' relative lack of confidence in discussing cybersecurity (Gale et al., 2022) leads to the lower prioritisation of cybersecurity being a standard-agenda item. This is not to say that boards do not appreciate the significance of it; rather, they are undecided on the way to proceed on it. One participant pointed out this failing by saying,

"The boards know that this is a big monster. But they don't know really what to do or what not to do. And security is even more complex. If the people have started understanding digital and cloud, then cyber security is at a different level altogether." - Participant 2

However, there are encouraging developments as well. In some organisations, the boards, increasingly aware of the risks and implications of cyber, are now associating specific individual targets with respect to progress on cybersecurity aims. Research also supports this view, increasingly adopted within the practitioner community using key performance indicators (KPIs) to stimulate contribution by security-relevant actors (Kosutic and Pigni, 2020). It is, in some cases, garnering as much discussion as may be devoted to other functions/operational subjects under the scrutiny of the board. One participant raised these points, saying,

"On the case of something like cyber security, five years ago, we didn't talk about it. Now we talk about it regularly and we'll have maybe a deep dive, as they call them, once a year. But even the KPIs associated with cyber security are part of the normal reporting pack now, and that wasn't before." - Participant 15

Overall, it is reasonable to remark that board engagement with cybersecurity has certainly increased in recent years. The appreciation of cyber risks and costs of cybersecurity investments, and discomfort around discussing cybersecurity has reduced and, together, these vouch for the requisite attention on this subject area from the governing boards, which it decidedly deserves. The next section discusses the insights that organisations have gathered through their experience which further help in confronting harsh challenges on the path to securing their organisational cyber realms.

4.5.2 Insights

Insights are the priceless learnings that organisations acquire through their previous experiences from having survived cyber incidents, which fuels their efforts to prevent future ones, or their appreciation of their peers' incidents (Ashraf, 2022) which drives their efforts to be more secure than what those peers were, or what they themselves used to be. Some of these are even realisations, which have arisen from years of successfully managing and preventing cyber incidents. Collectively, they are crucial towards strengthening an organisation's cybersecurity mechanisms.

4.5.2.1 Correct board language

In terms of popularity, one of the most significant and vital insights, as provided by some interviewees, has been the ability to articulate the risk, implications, and benefits of robust cybersecurity in ways that the board may be best suited to appreciate.

An interviewee astutely observed that one of the most elementary reasons limiting a board's engagement with these discussions is the challenge posed by the articulation of cyber risks to board members. Studies have indicated that this could be conducted by finding a lexicon common to the governing board as well as the leadership associated with cybersecurity, often the CISO (Cerin, 2020). This lexicon has been referred to as the risk management language as well. The view brought to light by the interviewee pointed out that,

"I know that from a cyber security perspective, engaging with the board has been a challenge for many, many years because of how hard it is to articulate the risk." - Participant 17

Research presents the opportunity offered by management in the form of a link helping governing boards assess (Landefeld, Mejia and Handy, 2015) and appreciate cybersecurity risks. In this study, another participant agreeing with the above scenario pointed out the importance of a CISO who can bridge the gap and help the board appreciate the risks emanating from poor cybersecurity, saying,

"The thing with boards is they don't understand technology, and sometimes they will get someone come in and the person doesn't really speak the language that the board understands. Virtual CISO or someone of that nature is supposed to come in and clearly explain how this technical cyber thing impacts your bottom line. He deserves your attention and resources. So, the other part of what I would strongly recommend is boards have to have the type of conversation and the input from someone who can put it in those type of terms." - Participant 14

Even the task assigned to the executive team responsible for cybersecurity (such as the CISO) is not straightforward, as it involves certain nuances unique to each organisation. However, there are reports and studies which can help CISOs through some essential guidelines (Allen et al., 2015). Meanwhile, some of the interviewees seemingly agreed that the reason for the CISOs' (or equivalent personnel in the leadership team) incapability to garner adequate budgets/financial support for robust cybersecurity mechanisms was largely owing to the board's inability to understand the essential concerns raised by poor cybersecurity. It was highlighted by one, saying,

"The CISO plays a very important part in conveying the message in an effective manner to the board. So, these guys are not IT guys, but they know what they're doing from a security perspective, from a board perspective, from a challenge perspective. So, she has the job of taking something that's quite technical and making it into plain English and reporting it, such that they understand. I think a lot of CISOs I've seen in the past… bless them they're IT geeks… they're very good at technology, but not necessarily good at presenting to the board and making

it easy to understand, and actually satisfying the board's questions with answers that make sense to them." - Participant 30

In several instances, the challenge is posed by the perception surrounding cybersecurity and its technological associations. Once the board members overcome that hurdle, they may discover that it is not actually so. One of the interviewees similarly opined that the challenge faced due to the technical perception of cybersecurity was unfortunate, as the technical association was merely a myth. This has been further substantiated by research supporting the realisation that this is, in fact, just a misconception (Boyes, 2015). They pointed out that,

"(Cybersecurity) people are a mix of... I guess kind of technical skills, management skills, communication, so being able to kind of communicate issues in an appropriate language. I mean again, it's kind of a cliche to say it at this stage, but it's a much more rounded profession than maybe people think. People just think cybersecurity is a very technical, geeky thing. It is absolutely not. There's a lot of complex social and organisational challenges to doing cybersecurity well." - Participant 23

Having overcome the technological perception of cybersecurity, the executive then needs to emphasise cybersecurity adequately so as to garner necessary financial support, yet not compel the board into feeling unnecessary panic. An interviewee was keen to point out that the appropriate way to gather the necessary budgets for cybersecurity from the board was to strategically draw their attention through the relevant association of cybersecurity and its business value to the organisation, saying,

"So, if you go into a boardroom and the first thing you lead off with is ISO 27,001, you've lost them. But what you do is you answer questions. If the question from the Vice President or a Chief Executive Officer is what security framework are we using? You say, 'Well, we're using ISO 27001, or we're using NIST 800 or we're using CIS 20' or whatever. But that stuff you don't start with. What you start with, 'These are the things that make us the most amount of money. This is the way they make us money.' ... that's the way of showing how the value of the company is created and how to protect that, which is how you make boards understand the importance of it." - Participant 19

The above views substantiate the considerable importance of articulating the risks and implications of poor cybersecurity in relation to the benefits received from robust systems to the governing boards, so that appropriate strategic focus is paid to this vital topic. Thus, the significance of appropriately articulating the risks posed by poor cybersecurity cannot be overstated. Identifying a language that the board is comfortable with (Cerin, 2020) and using it adequately to communicate the concerns, and erecting a robust cyber-defence system, is elementary towards making any progress in this regard.

4.5.2.2 People, processes, technology

This next subsection throws light on a term otherwise considered commonplace within the experienced practitioner community and, consequently, is crucial while exploring insights associated with robust cybersecurity governance mechanisms. Essential focus is to be placed on all three elements, rather than one over the other. While discussing the cyber-resilience aspect of cybersecurity, the above term gains more importance as all the three elements have a tendency to affect it (Boyes, 2015). The following comments explain the importance of the term and its significance on the path to securing an organisation's cyber realms.

One perspective is a combination of factors or resources (Barney and Clark, 2007b) being at the disposal of the organisation, which may be viewed as a unique dynamic capability (Teece et al., 1997) as well. This was highlighted by one of the interviewees who commented on the ideal IT function and the characteristics it ought to embody, saying,

"So, the IT functions do have a role to play. But the training has to be what is often talked about as a 'multilayer defence', which is - people, process and systems - and you need to tackle them all equally to make sure that your people have the tools… you need to make documented processes that are repeatable, so they know what they're doing, and you need to have a culture which says, 'OK, if you make a mistake/if you click on something/if you've done something you think it was wrong, tell us immediately, and there will be no consequence. We're here to support you, we're here to help.' and make that relevant." - Participant 8

This term gains particular importance considering that, in the field of cybersecurity, it is commonplace for the focus to be often misunderstood as one of the three. Consequently, organisations lack a cyber-secure system and either wonder why or are forced to learn the hard way (through cyber incidents). In certain instances, the focus may be on hiring adequate professionals to operate the technology. In others, priority is awarded to the technology and the IT systems themselves. This approach is flawed and then necessitates prioritising both the employees and the tools at their disposal (Wright, 2021). A participant emphasised this concept by highlighting the importance of placing both humans and technology beside each other, instead of under or over, saying,

"The idea is not to replace the human… it is an augment. The technology and human work side by side 'cause even from our perspective, we said we use huge amounts of technology - machine learning and the analytics - but we need the human layer, and you provide the context about what's going on, what to prioritise, what's new, and what's different… but you need both to work in unison. In essence, just can't just 100% rely on the technology as you can't 100% rely on the people." - Participant 16

The above statement gains particular importance in light of the fact that it is often believed within the industry that incidents happen owing to human error (Thackray et al., 2016). It then becomes especially significant to realise that strengthening the human element may add to the sturdiness of a robust cybersecurity system. This was mentioned by another participant in the following words,

"I have to be willing to ingest threat intel maybe a little bit differently or more proactively that'll give me a step ahead of these hackers. The goal is to get someone who has a more advanced way of thinking. Nothing could prevent the attack and then the other part again back to the users. Hackers generally write programs and exploit attack vectors in ways that, well, they know what we look for. The untrained technical person might be able to detect something that we may not. It's really quite possible that the attack can be stopped by disabling that user, that is launching all these processes you understand are associated with the ransomware attack, so it's really short-sighted to not invest in the users." - Participant 14

The insight from this comment underlines the research which draws on the significance of developing human capital within the firm (Banalieva and Dhanaraj, 2019) in developing firm-specific advantages. According to them, the managerial IT resource may be turned to, to extract the most value from modern technologies. This insight would support the potential of drawing a competitive advantage from this resource. It further goes on to support the concept initially highlighted (Barney and Clark, 2007a) by insisting upon the use of managerial IT skills as the one of the five attributes of IT which support its potential to be a competitive advantage.

Mata et al., 1995 in their discussion of competitive advantage from IT, also stress upon the management skills involved in dispersing information technology within an organisation. The views of Hsu and Wang (2012), which emphasise the collective knowledge and skill set of the humans as a resource, also support the view that individuals in organisations - and the way they use technology - make all the difference. The quote above, underscoring the reliance on people devising cybersecurity mechanisms, then supports this perspective of realising the benefit of humans and technology working in tandem, and not replacing each other. More and more, we find that technology can provide significant advantages to organisations, if they are handled well and uniquely by able managers, who exploit the advantages from it.

A few participants individually raised the importance of structuring processes around cybersecurity procedures as a vital component of robust cybersecurity mechanisms. This view is supported in literature as a unique and useful dynamic capability (Teece et al., 1997). These would invariably include processes which constantly monitor and scour the cyber borders for potential threats. Other processes meant to outline procedures - for when incidents occur - include incident response, business impact, business continuity (including continuity of operations (Boyes, 2015)), crisis management (Landefeld, Mejia and Handy, 2015) and other resilience plans. One of the interviewees articulated these thoughts, saying,

"Process is about having processes for following up, to make sure that your cybersecurity is consistently applied and understood within the organisation. Obviously, the people can change, they can move on, but ideally the processes within the organisation stay the same and evolve and are adopted or used… a good process that's followed regularly by people and evolves to work for the business and can be an enabler for that because it can reduce the uncertainty." - Participant 23

The report from Accenture (Accenture and Ponemon Institute LLC, 2010) previously highlighted the crucial cause of data breaches from lack of internal control and processes in place, thereby supporting the significance of adequate processes which support robust cybersecurity governance mechanisms. Considering the quote from the participant above, the views from (Klinke and Renn, 2006) gain special significance as they elaborate on required processes to manage systemic risks. Cybersecurity risks thus can be managed better supported by adequate processes in place to prevent incidents, and then resume function, should breaches have occurred.

These three terms complement each other and have the potential to create an effective defence (Michael et al., 2019) against most cyber-attacks. In the worst cases, when an incident has occurred, the emphasis of ‘people, processes, and technology’ should enable the organisation to resume function with the least inconvenience and damage to all stakeholders involved.

4.5.2.3 Elementary realisations

This subsection discusses a host of elementary realisations which were brought to bear as helpful for organisations to consider when creating their cybersecurity governance strategy. While they may seem simplistic, they also intrinsically point to the importance of common-sense solutions which help in creating secure cyber-defence mechanisms.

One of these was alluded to by multiple participants, stressing the value of the old maxim, ‘hope for the best, be prepared for the worst.’ In their opinion, the inevitability of cyber incidents was a given (Ablon and Libicki, 2015), so it was then incumbent upon boards and other leadership members to devise strategies best placed, to follow from that assumption, to reduce the damage and dysfunction.

“We as security professionals... most of us agree that a breach or an incident is a 'when', not an 'if'. So, it's a bit like Microsoft's concept of the assumed breach. Just assume that it's going to happen and then prepare. Now our take on it is that we're not 100% secure, and nor is anybody else. The NSA is not 100% secure, and they've got the words security and their ability in the title. So, we accept that, and we're mature enough to go. ‘It'll happen one day,’ but the important thing is your response. That is what you are judged on.” - Participant 21

Another simple yet vital element of cyber defence strategy, that has been highlighted, is the aim to be tough potential targets from threat actors who may be demotivated to attempt an attack when it is more painstaking than a standard case. This perspective was supported by a few more interviewees who voiced the importance of being difficult targets for hackers to breach. One of them simplified the reasoning using an analogy, saying,

“I guess they're looking for the easy target, so they'll probably scan everyone and pick the easiest one… so as long as you're not the easiest one. You know, I was liking it to where you live… if you live in a street of houses. We've got a dog and we've got a house alarm. So, if someone comes at the front door, dog barks and someone tries to break in the house, alarm goes off. So, because we've got those two things, in theory, a burglar is going to go for a house that hasn't got a dog and hasn't gotten alarm because it's easier, so he’s got those things. It automatically puts people off I think, and maybe it's the same for hackers. It kind of makes them, ‘you know what, we'll just go somewhere else 'cause it'll be easier’.” - Participant 20

Another insight which was voiced by many interviewees was the insistence on building resilience (Aldasoro et al., 2022; Premium Official News, 2022) as an integral component of the cybersecurity mechanisms of the organisation. Cyber-resilience was recognised a decade ago (World Economic Forum, 2012) as an important feature within the cybersecurity discussion, including within the practitioner community (Hubbard et al., 2021). Academic research also supports this insight, underscoring the significance of rigorous formulation of strategy and its continuous adjustment (Sallos et al., 2019) towards achieving success with respect to cybersecurity, which may also be considered a valuable dynamic capability (Teece et al., 1997) in the organisation's arsenal. One of the participants was quick to emphasise its importance with respect to the potential life of the business itself, saying,

"So, it has to be about business resilience. Absolutely. Cyber security is one of the number one risks that can bring your business down within seconds." - Participant 17

Mirroring the priority increasingly being given to proactiveness, as evident in practitioner's reports (Hubbard et al., 2021), another interviewee echoed this notion while pointing out that the increasing trend amongst cyber-aware organisations was prominent in their human resources, with the following words,

"I think you've got some CISOs (who) are now changing into Chief Resilience and Security Officers as well. So, it's moving it from that reactive state to proactive." - Participant 16

These comments drawing this section to a close highlight a few essential learnings which, together, begin to outline elements of a successful cybersecurity strategy. The next subsection discusses another implement - regulation - which is necessary in creating a robust cybersecurity strategy.

4.5.3 Regulation

This section highlights another important tool, helping to confront several cybersecurity challenges which were explained previously in section 2. In the 4.0 economy, the cyber realm is challenging to secure, but this section entertains the notion that regulation may be one of the key implements to support that objective. Perhaps, a potential solution to the cybersecurity problem may even lie within policies (Mulligan and Schneider, 2011) or regulations framing the area. This section thus explains the role regulations play in helping organisations secure their cyber landscape, sometimes enthusiastically, while others reluctantly.

During the interviews, the conversations centred around regulations invariably pointed out the impact GDPR (General Data Protection Regulation) has had in the UK and European Union in recent years. According to them, GDPR's obligations to incorporate security controls placed on organisations (Michael et al., 2019), with the risk of facing substantial fines for failure to do so, have compelled even cyber-unaware organisations to be concerned about cybersecurity. This is also supported by academic research, pointing out the significance of regulatory actions - like GDPR and SEC (Security Exchange Commission in the U.S.) Guidance on Public company disclosures - in accelerating the trend (Nolan et al., 2019) of and need for cyber reporting (Cristea, 2020; Kiesow Cortez and Dekker, 2022). One of the interviewees articulated these thoughts saying,

"I think for CNI (Critical National Infrastructure) in the US, it's mandatory to have a CISO have that position. I think it is by law. I don't think in the UK, it is yet kind of gone to that level. So, in short, I think these are the things driven by guidance and regulations and compliance. Compliance is actually a big part of it. Isn't that GDPR's rule: for any kind of data leak, if it is seen that the company hasn't invested in proper security controls, they can be fined up to 3% of their revenue? Yeah, so there you go, that's GDPR rule. So, it is a compliance issue. It's kind of boards' imperative." - Participant 22

Speaking about compliance, a few interviewees highlighted the focus it received on account of being a part of certain industry sectors which are regulated by the government. Since the financial sector is increasingly targeted by cyber criminals for financial cybercrime (Nicholls et al., 2021), the banking and financial services sector has always attracted regulatory activity. Even in the case of financial cybercrime, regulations exist, which require member organisations to follow certain actions regarding both protecting data and reporting cybercrime (Kiesow Cortez and Dekker, 2022) in some cases. Thus, the sector necessitates a level of compliance and regulations (Landefeld et al., 2017) which the businesses have to observe to function within all those specific sectors. From one perspective, regulations may also be considered an intangible asset or resource for the organisation, which would allow associating the notion of deriving opportunities from it later in time. One of the interviewees highlighted,

"... depending on the business, what are the laws that regulate how you do what you do. So, in Ireland, insurance companies are very highly regulated. There's a lot of legislation, so we have to employ a team of compliance. Their job is to read all the law and make sure we're doing everything properly and make sure that you remain compliant. So, it's actually a big

part of the business. I think the whole compliance is often seen as a kind of a sleepy kind of backwater, you know. Increasingly (in) certainly insurance... and probably financial services... it's (compliance) a key part of the business now." - Participant 20

In terms of sectors which have to observe compliance to laws and regulations mandating certain cyber security procedures, one of the interviewees pointed out the contractual and ethical obligations faced by the technology industry. This industry has been found by researchers to be higher on the curve, demanding board-level cybersecurity effectiveness programs (Morrison and Kumar, 2018), highlighting the board-level interest in cybersecurity best practices. It further supports the needs of the technology industry, even with regards to cybersecurity regulation. They collect volumes of customer data and are then required to follow several guidelines to protect the data to the best of their ability. They said,

"There's something in English law called Duty of Care. So, the simple fact of matter is that we have a duty of care to do everything under our control to make sure that we don't create vulnerabilities for customer. So, when we're signing large contracts with customers, we take massive amount of liabilities… and these are all contractually hardbound in the way in which our relationships work. So, we don't have the luxury of even thinking about not being serious about this topic… because it's a binary issue. If you are negative on this issue then you're out, simple as that." - Participant 2

Scholars have identified four main types of organisational response to cyber breach incidents and their disclosure. Abraham and Sims (2021) highlight that there are four prevalent kinds of organisational culture-to-cyber incident-disclosures: (a) ignorance/neglect (b) defiance/complacency (c) compliance (d) integrity. Among these, the last one - integrity - is displayed by an organisation with a strong HRM and Information Security Leadership, who are prominent advocates for the disclosure of such events.

Other conversations discussing regulation had a futuristic perspective, with respect to what should be brought in, and what may be likely to be included at a future date; this has even been stressed in recent studies. They point out the importance of publicly disclosing cyber management failures (Nolan et al., 2019). Beyond this, there is also the adverse impact of cyber-breaches in the form of reputational (De Minville, 2020), financial, and legal losses, which an organisation has to bear and is well-known. Relatively less concerning is the impact on the employees who undergo substantial distress. One participant alluded to this distress possibly being covered under future regulations, saying,

"Maybe it'll emerge, especially in U.S. law where you can sue for anything, that the failure of the Board of Governors to direct cybersecurity, led to the extraordinary stress and health problems of the line staff responding to that data breach. Perhaps there is a whole workplace health and safety aspect to data breach governance that we haven't explored yet under law, but I could see it emerging definitely as a future trend... what they call it in the United States... it's like intentional infliction of stress, I believe. You can sue the person for doing that to you."
- Participant 19

One of the interviewees hinted at expecting more support from the government, which required organisations to disclose information about breaches they suffered - which would enable others in the industry to observe, learn, and possibly prevent them, in turn. This reporting of incidents and understanding of inherent risks (Kiesow Cortez and Dekker, 2022) involved considerable support, developing the situational awareness of the field through public and private reporting mechanisms (Mulligan and Schneider, 2011). They articulated these thoughts by bringing an example of a different country, saying that,

"There's Australian Government (who) are also planning -I don't know if they've put it into motion yet - but they did raise a white paper or parliamentary discussion on having to inform the Australian government before paying ransom for ransomware attacks. That is another angle because ransomware is out of control and it just seemed to be such an effective tool at making some people very, very rich… I think in terms of government, they should always be doing more, and it could be at the small business level all the way to the large organisations. I think (we need to) put things into law and force them (organisations) to, they were saying, discuss and talk about these breaches." - Participant 27

Another interviewee, who came from a position of authority within the government, was able to throw light on the new regulations the government may be keen on bringing into practice, in the near future. Research has outlined the need for law to support initiatives in the field of cybersecurity (Mulligan and Schneider, 2011). Existing law or potential future laws ought to insist on creators, producers, and manufacturers to incorporate security in the products and services they eventually sell.

"There is no obligation to report a major cyber incident to the regulator unless you're in financial services. So, if you're in financial services, it's different 'cause of the FCA regulations, by the listing rules - also run by the FCA. By the way, the listing rules don't require non-financial services to do anything about it. So, it does come down to the transparency of disclosure that they want to give to the marker. Auditors generally don't comment on that in their audit reports, and we are working on how transparent an auditor's report about risk is."
- Participant 31

These comments from the participants indicated that regulation, while not a popular move of the authorities, invariably has led to organisations in certain sectors to be more vigilant about planning and implementing adequate cybersecurity procedures. They alluded to a potential near future where those currently under no legal obligation to report breaches or follow other regulatory (Kiesow Cortez and Dekker, 2022) procedures may not have this luxury anymore. Cumulatively, it may act as a move in the correct direction, as far as strengthening the security of the borderless and intangible cyber realm is concerned. In any case, the evolving digital realm necessitates an evolving legal landscape as well (Bejan, 2022), in a bid to prohibit and sanction criminal cyber behaviour.

4.5.4 Summary of Theme 3

Highlighting the challenges in Theme 2 has been instrumental in emphasising the insightful ways to overcome those challenges which an organisation encounters on their path to robust cybersecurity. These tools to confront the challenges are diverse, yet together possess adequate power to equip an organisation with necessary weaponry to create a fortified cyber realm. Engaging the highest echelon or the corporate pyramid in vital cybersecurity discussions, incorporating meaningful insights from past experiences and complementing relevant regulations are, thus, effective tools. The next theme calls attention to the opportunities available to the organisation to ensure robust cybersecurity.

4.6 Theme 4: Advantages from Robust CS

The previous sections outlined the challenges borne by organisations on the path to securing their cyber space, as well as the ways in which they set out to confront those challenges. As they conquer those problems, there are varied advantages which culminate from being able to implement robust cybersecurity mechanisms. This section explores these two advantages - namely, competitive advantage and organisation-specific advantages - in detail.

4.6.1 Competitive Advantage from Robust CS

One of the most significant advantages of experiencing a fortified cybersecurity procedure is the potential to derive competitive advantage from it. It may seem fantastical to imagine deriving an advantage over competitors from the correct deployment of cybersecurity, while visualising it as erecting a boundary wall for threat actors to scale. But the connection lends itself credit from first understanding what a robust cybersecurity system is protecting. Cyber-assets could well include a range of data and information owned by (or under the protection of) the organisation, which may belong to any of its stakeholders - customers, employees, business partners, etc.

All this securely protected data is a key resource for the organisation, which has the potential to provide a new kind of competitive advantage (Abraham and Sims, 2021), especially in a digitalised era where cyber events are increasingly common yet complicated. Increasingly, research attests to this view and supports the idea that cybersecurity can improve competitive advantage (Kosutic and Pigni, 2020). The conversations with participants explored various aspects of advantages, in general, and the way these could provide advantages over competition, in particular.

Multiple interviewees broached security as a high value item sought by an increasing number of customers which, if provided by the organisation, allows it to enjoy an advantage of being preferred over its competitors, for providing this essential feature. Even research has corroborated this trait of protection of consumer data leading to trust, which further enhances corporate reputation (Corradini and Nardelli, 2020), thereby leading to one resource acquisition of another intangible resource (Barney and Clark, 2007b; Rindova et al., 2010) valuable to the business. One of them articulated it in the following words,

"In a world where you're handling personal data in order to conduct business, if you're in a competitive market, it is to your advantage to be able to say, 'You can trust us with your data, and here's why you couldn't trust them with your data.' And I think it is potentially a competitive advantage to be able to pitch somehow that you will protect their information, that it's handled in a certain way you know, etc. I might be out of date, I don't think there's a sort of certification process in some way you could say, 'Oh, I'm a level 5 and they are only level 3, so it's safer with me than it is with them.' I'm not aware of that, but it seems to me that it would be a competitive advantage at the margin if all it does is get you another 1% or 2%." - Participant 31

On several occasions, the priority to cybersecurity measures is propelled by the cyber-aware end customer (Wright, 2021) who could only be convinced to purchase a product which provides adequate security as a default feature. In the study, a participant indicated that an insistence of providing a cyber-secure service or product is being necessitated owing to the increasing levels of awareness of the customer, saying,

"And they're (customers) asking some quite detailed questions, and this is telling me that the customers are putting security right at the very front and centre of their thinking when they're onboarding a new supplier. The wider customer base, the marketplace, if you please, is now becoming increasingly conscious of security risk. It's not everywhere, don't get me wrong. But certainly, what we're seeing is that if we don't tick the boxes around security, we're running a real risk of not winning the business." - Participant 21

Another perspective was offered by an interviewee who pointed out the potential to derive a competitive advantage with respect to the sector an organisation may be functioning in. According to them, the sectors associated with high risks/ threats at the hands of criminals would understandably gain a significant advantage from incorporating tough cybersecurity measures. They said,

"So, we can show that, for example, the new military vehicle that we are producing on the new ship that we're constructing, that's much more cyber resilient - so there we use the term cyber resilient - than our competitor, and there is a way to prove that then… that immediately becomes a competitive edge. That's now a competitive edge at a national-level event, right? So, there are different levels of it. I think the case to use it as a competitive edge will differ as per the nature of the business - the businesses that are in the business of protecting their end-customer, whether it's them, or whether it's their data or whether you know how much valuable information they hold up." - Participant 22

Another participant mirrored the thoughts about competitive advantage being possible, depending on the nature of business and the extent to which it relied on technology. It further highlights the significance of building a culture on the foundation of sturdy cybersecurity, fuelled by digital resilience (Premium Official News, 2022). This view aligns with literature which supports cultivating high-level processes to serve organisations as dynamic capabilities (Teece et al., 1997), as well as reconfigured resources that are challenging to imitate. They implied an insistence on resilience as well, to be able to derive a real advantage from it, saying, *"Technology, to be a competitive advantage, has to be dynamic in nature. This (means) constantly evolving and being adapted to changes that are happening. And also depending on how involved IT in your company or technology in your company is. Is it the core running for the business or is it just storing data or whatever it's involved in, whatever degree of involvement it has, and then you decide how to make use of it."* - Participant 15

The discussion for deriving competitive advantage from robust cybersecurity further led to a curiosity of the way to be able to demonstrate or establish it without any reservation. Considering competitive advantage for each organisation is also a perceived advantage, which sometimes may be challenging to approach in tangible terms, in addition to protecting the data or the stakeholder information - the crown jewels (Hubbard et al., 2021), so to speak. To this, an interviewee suggested a simple exercise, saying,

"It depends on the sector, of course, but if I'm a client and I'm giving you my data, I don't just want to know that you're ISO 27,001 certified, or that you've got a CISO who's come to my organisation and told me how amazing he or she is, and the board take it very seriously. That's great. I expect you to do that because I'm investing millions of pounds with you, and I'm giving you my crown jewels to look after… I suppose they could actually tangibly measure and then realistically state those facts." - Participant 27

Increasingly, conversations in the boardroom and leadership tables in organisations and governments touch upon incorporating security and privacy (Michael et al., 2019) in the product/service offering. A participant from the interviews, was able to offer clarity from his end about the way an organisation could stake the claim about security as a component of its product/service offering. They said the following,

"I wouldn't necessarily say that you put it on the front page of your website and emblazon that everywhere. But certainly, the badges like Cyber Essentials, ISO27001… organisations do have that on their websites, and it does show that they are serious about things. But certainly, when you're having face to face conversations with your prospective clients, that should definitely be the time when you push it and you make it very clear that security is a key part of your strategy, particularly if you're a data company. And it is something that you have that competitive advantage with." - Participant 8

Understandably, however, if organisations stake that claim, it might inadvertently also invite the attention of threat actors who may want to challenge the organisation's assertion. We discussed previously in 4.4.2.2.3 that criminal motivation (Chng et al., 2022) to derive financial benefit, or even the accomplishment of breaching an organisation's cyber boundaries, can prove counterintuitive in relying on the strength of cybersecurity. In such a case, one of the interviewees' thoughts offered an insightful relief, when he said the following,

"If you're the hacker that says, 'I broke the FBI,' there's something to it about the challenge of it. I think particularly, if you handle large amounts of money, you are definitely making yourself more of a target. But remember, you're also in a stronger place than other people. So, although there's some criminal elements (who) will target you because you're financial and you're large and you say you're good, most criminals - in my experience in (government ministry) - most of them will go for the easier hit." - Participant 31

The above conversations largely point to the considerable potential in deriving competitive advantage from robust cybersecurity, in certain sectors and by certain organisations, if they are strategic in their approach to it and observant in the way they articulate it in the public eye. This revelation is significant in the 4.0 economy, where many businesses are struggling to manage the otherwise overwhelming aspects of digitalisation and protect their borderless cyber realms. The next subsection explains the other advantages which accrue from robust cybersecurity governance mechanisms.

4.6.2 Organisation specific advantages from robust CS

So far, we have discussed competitive advantage as a significant potential advantage accrued from a fortified cybersecurity measure. However, there are other considerably valuable advantages which can also be derived from robust cybersecurity. These three are a collection of tangible and intangible advantages, which are discussed in the following three sub-categories.

4.6.2.1 Trust

Organisations need to nurture the trust of all their various stakeholders in order to stay in business. Literature has simultaneously underscored the value of stakeholder trust as an important resource (Barney and Clark, 2007b) to organisations intending to augment their business value. Especially their end-customers - to whom they are providing the service or product - need to be assured of security, as they give their information and money to the organisations based on the latter's request. Whether it is a single sale or repeat business, trust acts as the foundation for them. In businesses where customer information is sought, the underlying customer assumption is that the business (such as a bank) will protect their information (Wright, 2021). One of the interviewees articulated this elementary need for a business to win trust by offering security, with the following words,

"… for example, organisations like, say Tesco or John Lewis, are trusted brands. So, when you are providing your card details, you are comfortably providing those. But if it's other organisations, maybe say in London where you shop locally, it has a website and asks you to provide those details… you'll think twice, isn't it? So, it's all about building trust with your communities." - Participant 18

Research is increasingly relating the use of ethical digital practices with increased customer trust, especially where customer data/information is involved (Wirtz et al., 2022), as previously mentioned with corporate digital responsibility (Lobschat et al., 2021). Reports confirm that transparency is the key to customer trust (Cisco and affiliates, 2023), which is a valuable resource (Barney and Clark, 2007b) - and being transparent with how customer data is being used and processed is a step in that direction. Another interviewee voiced similar opinions, emphasising the importance of being able to secure the trust of the customers with the following words,

"I say it's all about the trust. So, you're kind of saying, it's really important that I don't just give you this product, with no security whatsoever. You know the first time you use it; your data is exposed to the Internet and every man there (is out for) stealing it. 'I'm not gonna buy it. I'm not gonna use that again. You know that company is in the media for the wrong reasons.' That's why there is a real business benefit and value to doing this (cybersecurity) by default and design." - Participant 16

Good cybersecurity practices can also pave the way for enhanced trust from various stakeholders, including regulators, business partners, investors, and customers, which is a precious resource (Barney and Clark, 2007b) for the organisation. Research highlights the increased trust emanating from opting for independent cybersecurity attestations (Morrison and Kumar, 2018) by organisations. An interviewee suggested that this trust is not only sought from the customers but, in certain cases, also from the authorities with which the organisation has to work, saying, *“If you think about why organisations invest money in cyber - they will do it because they want to be trusted. They want to kind of achieve that kind of customer trust and the trust of the regulator, right?”* - Participant 24

Practitioner reports second this opinion (Premium Official News, 2022) highlighting the trust as the cornerstone for financial organisations (Browdie, 2013), which is, in turn, enhanced by fortified cyber defence systems. An alternative way of viewing this is by taking the case of incidents. The reason certain cyber breaches have the potential to shut down the organisation is owing to the loss of trust from the customer, who is unable to feel secure with the organisation again. From this perspective, not organising robust cybersecurity can lead to an eventuality wherein there is an absolute loss of customer trust, overnight. It is, thus, imperative to view stakeholder trust for the valuable resource (Barney and Clark, 2007b) it evidently is for the organisation. One of the interviewees astutely pointed out,

“It is an entity-level ending event if you have a major breach. And not just that, what happens with the regulator/the ICO and all that kind of stuff – it is people's trust in your organisation 'cause you lost their data. So, it plummets, and they won't give you their business. ‘I'll go somewhere else’.” - Participant 31

Therefore, either perspective of attempting to win customer and other stakeholder trust (De Minville, 2020) or not wanting to lose it, provides adequate impetus to realise the linear association of robust cybersecurity’s role in cultivating and retaining stakeholder trust. The next subsection explains a similar benefit arising from a fortified cybersecurity system in the form of a dazzling reputation.

4.6.2.2 Reputation

Organisations strive to build great names for themselves, over the life cycle of their brands, so as to be able to derive other advantages from this. A great reputation, like trust, is slowly earned (De Minville, 2020), and while it cannot be cultivated overnight, it certainly can be lost quickly if the organisation does not adequately protect its assets. Thus, in instances of cyber breaches, the reputation, once tarnished, may either never be reclaimed, or at least may take years (Nolan et al., 2019) and concentrated efforts to recover. Meanwhile, the ability to plan and implement a robust cybersecurity governance (von Solms and von Solms, 2018) mechanism allows the firm to enjoy the advantage of augmenting its reputation.

Research points to the direct link between strong cyber defences and an upright organisational reputation among its varied stakeholders (Corradini and Nardelli, 2020; De Minville, 2020). One participant was keen to highlight the importance of cybersecurity governance in its impact on organisational reputation, which takes several years to cultivate (Mata et al., 1995). Even literature supports the view of reputation as an intangible asset (Rindova et al., 2010) or resource (Barney and Clark, 2007a; Peteraf, 1993) of the organisation, which may only be cultivated over the long term. They articulated these thoughts in the following words,

"For us, it's all about looking after your clients and your reputation. We spent 20 years building a good reputation. One bad thing can destroy it… there's a necessity, let's say, from a reputational perspective, to be able to protect all this stuff. I think the same with banks looking after people's money and bank account details. So, if you're not on the ball when it comes to security, you're not going to survive 'cause sooner later something will happen." - Participant 20

Literature highlights the strong association between risk construction and its impact on the reputation of an organisation (Kewell, 2007). In the context of individual leadership within the organisation, this impact may be magnified. An astute observation by the previous participant explored this different perspective. Mirroring the findings from literature which support the risk of personal liability of directors in case of data breaches (Landefeld et al., 2017), they hinted at the impact on an individual board director's reputation when a cyber incident happens. They pointed out,

"From a personal perspective, you know as a director of the board, if something does go wrong, we can't necessarily stop it going wrong. But after whatever has happened, there will be some kind of post-mortem or review to say, 'OK, why did it happen, what were the reasons?' And if you individually as a director and collectively as a board can say, 'Well it did happen, but we had all these policies and procedures in place which we followed through and we gave everything due consideration, and it still happened.' you know you're less liable as an individual and board." - Participant 20

Another interviewee pointed out the overall impact on an organisation's reputational perception as a resource (Barney and Clark, 2007b; Peteraf, 1993), which is also vital to its business function. Even research corroborates this view, highlighting the direct association between negative cyber events and adverse effect on organisational reputation (Gale et al., 2022), including impacting its shareholder activity (Tosun, 2021). Some scholars have emphasised the further impact of a strong reputation on the ability to mitigate unwelcome events (Kewell, 2007), which makes for interesting notions to explore in the context of cyber incidents. The reputational damages are difficult to quantify (Aldasoro et al., 2022) but significant, nonetheless. They pointed out the challenge of making amendments to their routine as a result of increasing cybersecurity procedures, while drawing solace from its impact on the organisation's cyber perception. They said,

"We're now looking at things and we're documenting better… our policies and procedures, we're going through the whole SOC2 and ISO 27001 and all that. So again, that's forcing us because they work in the banks, it's a bit of a pain, but if you got it, it is what it is and it shows to the world at least you got a basic level of whatever (cybersecurity)." - Participant 10

An organisation capable of building and maintaining a strong perception with respect to its cyber abilities has a natural advantage in upholding a good reputation. The above comments cement this perspective, while the next subsection explains the advantage an organisation derives in the form of increased business and revenue growth.

4.6.2.3 Business growth

Business growth and a boost in organisational revenue may be considered the most significant and popular objectives of any given business. Poor cybersecurity posture leads to exposed vulnerability leading to cyber incidents which, reports confirm, ultimately leads to poor business performance (Corallo et al., 2020). Perhaps, it is reasonable to conversely believe that a robust cybersecurity system would allow the garnering and/or augmenting of the business growth/performance. This is further revealed through the comments of interviewees in the following subsection.

One of the participants observed that good cybersecurity enables the business to then sell on other virtues, once their security is assured. Being a Business-to-Business (B2B) organisation, as opposed to a Business-to-Customer (B2C) that sells its products to financial institutions, they believed in the vital importance of security as a basic step in making a sale. Identifying a cyber-secure product as a valuable resource (Peteraf, 1993; Wernerfelt, 1984), enables opportunities associated with business growth consequently. They articulated these thoughts in the following words, *"It's something I don't have to then convince them of. So, it just becomes a hygiene factor that says, 'We are who we say, we've done this, and you don't have to worry about it.' I want that just to be so we can then sell on the functionality… on the benefits of how we can help the banks be more innovative and do stuff, and this security layer underneath is just a building block that's there. The foundations are strong and then we sell on the other stuff rather than on the security."* - Participant 10

A different interviewee viewed it as a way to make a sale to the potential customer by demonstrating their compliance with regulations and assuring their clients of the implied security in their product/services. According to them, apart from being a cost to the business it also offered benefits, saying,

"So, if you do it well, it actually benefits the business. It is a cost to the business, yet, if they do a good job in terms of compliance and all the different aspects, it should make the business run better and it should make it easier for you to sell your business to clients. So, if you can say to them, 'These are our certificates to say we're in full compliance with everything.' They are reassured that you're doing everything properly. And it isn't (just) cost, but it should be a benefit as well." - Participant 20

Another perspective to business growth through robust cybersecurity is through exploiting the benefits of digitization, which is a valuable resource (Barney, 1991) capable of enabling advantages over rivals in the course of operating the business. Identifying the impact of global external factors on the choices made by businesses, as an effective practice, a participant explained it in the following words,

"I think covid's been a good accelerator of this, as they want to take advantage of the benefits that digitization brings. And if you can reduce your IT cost and you can make people work more efficiently, then you'll make more revenue. One way you do that is by sticking all of your data in the cloud, and making everything open, which creates a different security paradigm. So, I think cyber security is an enabler which allows you to get the financial advantage of digitalisation." - Participant 24

Another perspective highlighted the significance of learning from past and peer experiences in the aid of avoiding major cyber incidents in the future. A participant viewed it as an evolutionary advantage over one's organisational competitors, when they are able to conduct the basics of cybersecurity adequately, whereas many of their peers are not able to guarantee the same - highlighting the need to learn from unfortunate peer incidents (Ashraf, 2022). They commented that,

"So the advantage of having a system that's clean and isn't constantly being attacked left, right and centre, means that you are in a space where you can guarantee the security of whatever the business function is that you're performing for your customers, which again inspires customer confidence and allows the growth of the business in a way that would not otherwise be possible if you had poor security. And the risk of suddenly going out of business or incurring massive costs as a result of a security incident is greatly diminished. So, by doing the basics well, you actually put yourself at an evolutionary advantage above other companies that are in the same market as you, that are not doing the same." - Participant 25

These comments support the view which states the advantage of business/revenue growth from incorporating robust cybersecurity procedures. Whether as a necessity to secure more customers, or retain existing ones, this advantage is of great importance as it also tends to differentiate an organisation from its peers who are as yet struggling with implementing a tough cybersecurity system. The next section explains the theme that emerged purely during conversations with participants about those organisations, which may be considered successful in implementing the adequate mix of all cybersecurity governance mechanisms.

4.6.3 Summary of Theme 4

This theme has highlighted several advantages that organisations may be assured of once they are effectively able to secure their cyber realms. These advantages understandably accrue from various other organisational practices and sources as well. However, in the context of this study, and having employed the tools to confront challenges (as discussed in themes 3 and 2, respectively) they are able to derive the same from robust cybersecurity. While trust, reputation, and business growth are significant advantages on their own, a cybersecurity-led competitive advantage is a unique learning from this study. The next and final theme examines those particular organisations which have been able to hone their cybersecurity mechanisms to such a degree that, internally and externally, they are being perceived as winners.

4.7 Winners

While literature may not express this category in a similar fashion, the interviews with the participants were revelatory in articulating the category of organisations which have understandably emerged victorious in implementing (Barnes, 2019) apt cybersecurity procedures. Some researchers have delved into the cybersecurity wellness of organisations in certain industries (Critical Infrastructure) and proposed measuring it through vital signs (Jazri et al., 2018) associated with cybersecurity. This may be a fresh perspective on organisations supposedly *winning* in the cybersecurity arena. Using a combination of continuing function, retaining stakeholder trust, and upholding sparkling reputation, these organisations evidently are privy to certain secrets which the rest of the industry is not privy to. This section explores the features of such organisations and the way they achieved the winner label.

In previous sections, we found comments highlighting the importance of cybersecurity for sectors which are highly regulated, and thus enjoy the advantages which accrue from those. However, one of the participants perceptively noted that certain organisations, which are able to approach it holistically, may derive significant benefits, perhaps even more so than organisations in the regulated industries, as they are being compelled to follow it. They said,

"So, I think that's what I would say is other organisations who are embracing it more, who haven't necessarily had the regulatory burden, and who are perhaps not as advanced and mature as some of the other industries. They probably are on par or even ahead of some of those highly regulated industries, so I think it really comes down to the approach. You are embracing it holistically as a business initiative, as a business opportunity, as a business risk. And looking at it basically as people, process, and technology… holistically. That's really, really important." - Participant 17

Another participant viewed this category as a combination of organising a few things simultaneously; incorporating a resilient system with constant threat awareness would make an organisation more successful than others. This insight is finding support in multiple practitioner reports as well (Hubbard et al., 2021). This may also be a moment to identify this perspective of the combining of resources and/or simpler resources, which may then be viewed as a dynamic capability (Eisenhardt and Martin, 2000; Makadok, 2001; Teece, 2007; Teece et al., 1997; Zollo and Winter, 2002) specific to the organisation. This view also includes employing a *stewardship* trait (as a complementary behaviour to other best practices) amongst employees, who go above and beyond the organisational security policy (Ogbanufe et al., 2021), in order to secure the cyber realm. Furthermore, associating the *win* with being able to thrive in an uncertain cyber-reliant future (Abraham and Sims, 2021) may be considered another advantage of a proactive and forward-looking cyber stance. They articulated these features by saying, *"Yes, if somebody is able to have very strong security controls, has invested in a really good threat intelligence, constantly does threat assessment, has all kinds of security solutions and can show how secure they have been, then definitely should be talking about (winning)."* - Participant 22

Incorporating cybersecurity, privacy, and data rights into the design process (Cisco and affiliates, 2023; Michael et al., 2019) is not a novel conversation, having been explored in academic works. Furthermore, using the new technologies - like machine learning, artificial intelligence - to strengthen cyber defences (Cristea, 2020) may be considered a worthy enterprise. From the interviews, another participant seemingly mirrored these sentiments by extolling the virtue in constantly maintaining systems which enable robust cybersecurity by saying,

"What we can only assume is that they've got very good teams who are constantly maintaining everything they need to maintain. And it is a constant maintenance thing." - Participant 8

Reconfiguring resources into routines (Eisenhardt and Martin, 2000) or integrating the practice of building such internal processes to address the changing external environments (Teece et al., 1997), have been identified by literature as dynamic capabilities.

Thoughts similar to the above interviewee were expressed by another interviewee, who stressed on the importance of reaching a point of secure cyber realm; however, instead of relaxing from that perch, to be constantly working and maintaining that fortified system of cybersecurity. Scholars point out the requirement of comparing the current state of cyber-preparedness to a future state of preparedness that may be necessitated (Cristea, 2020). This could offer great insights in organising the processes required to prevent, protect, and prepare the adequate responses. This, in itself, may be recognised as a valuable dynamic capability (Zollo and Winter, 2002) of the organisation, with respect to its IT routines and processes. The interviewee said,

"There's absolutely an answer there… if the business wants to do that, then there's absolutely the answer - a totally secure cyber security system. But I think that to get to that point, it's got so many different elements to it… so can you get to that point? Yeah, you can absolutely get to the point… but in order to get to that point, you need to be understanding exactly where you are at a point in time and then to continually update and audit where you are at." - Participant 27

The other views centred around the significance of focussing on incorporating security as an elementary feature of their end product/service. This holds true for most organisations whether or not they are involved in selling security as their product or service (Kosutic and Pigni, 2020). One of the participants articulated their thoughts, saying,

"I do think that we're only gonna go - I hate to use the expression - we're going to win this. We're going to get ahead by building products where security really is there by design." - Participant 29

As pointed out previously, when viewing cybersecurity as a resource, this perspective of reconfiguring it into a routine that enhances the use of the resource, is a distinct dynamic capability (Eisenhardt and Martin, 2000). Similar to this comment was another interviewee's opinion which emphasised organisations that appreciated the burden of being able to secure customer data and justifying their trust in protecting their information (Wright, 2021). This could be viewed from the CDR perspective as well as from the one mentioned in 4.3.1.2, pre-supposing customer data privacy and protection as a guiding principle for CDR (Wirtz et al., 2022). They pointed this out by saying,

"If there are people, companies who are responsible and trustworthy doing the right thing and put in the controls... they're the ones who I think will win ultimately." - Participant 16

In contemporary times, when information is as precious as gems, being able to secure these gems/crown jewels (Hubbard et al., 2021) offers unique opportunities to appreciate an advantage over the organisational competition (Abraham and Sims, 2021). The above comments may be surmised to understand that there is often a combination of factors which are likely to enable an organisation to 'win' at securing robust cybersecurity measures, which may provide a potential competitive advantage. These factors are, however, unanimous in their insistence on preparedness, resilience, and working with an objective of gaining and maintaining stakeholder trust. Thus, cybersecurity, as the most discussed topic of the 21st century (Cristea, 2020), may very well be so in a more encouraging manner than being often necessitated by unpleasant dialogues.

4.8 Surprising Theoretical Finding

This study led to a surprising yet unequivocal finding, which led away from the initial premise and path opted for in this research. During the phase of literature review, the importance of the board members' stewardship role, which enables them to embrace a mentoring stance, was considered to be the impetus for robust organisational cybersecurity. Having discussed this role in 2.2.4.1.6, the supporting theory was apparent in the form of the Stewardship theory (Donaldson, 1990), as examined in 2.6.2. However, through the course of the data collection, and consequent data analysis and discussion, it became evident that the research had extended into a divergent direction which did not perpetuate the given premise. Instead, it examined the potential for cybersecurity as a resource which enables the organisation to exploit opportunities including advantages over its competitors. Hence, the findings led to novel and unexpected insights, which have led to the development of associated propositions.

Thus, while the research initially started with the premise of the significance of stewardship, and support of theoretical foundation in the Stewardship Theory (Donaldson, 1990), the data collection and analysis, diverged into the significance of intangible assets and the perspective of viewing them as potential sources of competitive advantage, and dynamic capabilities. Hence, the contributions to theory from this research (as detailed in 5.6) is thus to Resource-Based View (Wernerfelt, 1984) and Dynamic Capabilities (Teece, Pisano and Shuen, 1997).

4.9 Chapter Summary

The discussion of these 5 themes brings this chapter to a conclusion. The five themes emerging from the primary research data are able to demonstrate the various factors influencing organisational cybersecurity choices, which are then further challenged by several external factors. This study underscores the practitioner experience to examine appropriate tools for confronting those challenges while on the path to robust organisational cybersecurity. The organisations capable of emerging victorious over the challenges enjoy certain advantages, and a few amongst them are even fortunate enough to emerge victorious amongst all - rivals as well as threat actors. These have been explored in this chapter. The following chapter would conclude the thesis while demonstrating the model and propositions emerging from these key themes.

CHAPTER 5: Conclusion

5.1 Introduction

This chapter forms the conclusion of this thesis and presents the findings from the data collection, analysis, and discussion. It leads with a summary of findings from the data analysis, which further leads to the development of a model that explains the inner workings of an organisational path to robust cybersecurity and the way it could potentially enable a competitive advantage. The assessment of quality of research is evaluated next, followed by an examination of the achievement of aims and objectives which this research sought from the beginning. It then leads a discussion of contributions to both theory and practice, through this emergent model and discussion. Furthermore, limitations to the research are then highlighted, in addition to the avenues for further research. The final element before concluding the chapter is the researcher's reflections through the doctorate journey, which draws the chapter and the thesis to an end.

5.2 Summary of Findings

The previous chapter detailed the analysis and discussion of the collected first-person data, which brought to the fore five main themes. These themes are now summarised in the context of emerging inter-relationships and findings from the study.

The first theme focusses on a collection of organisational features which together impact its stance on cybersecurity. These are primarily under two main sub-themes, namely: organisational characteristics impacting cybersecurity needs, and organisational decision-makers for cybersecurity. The former sub-theme is vital in influencing the organisation's need for a reliable cyber defence mechanism through its cybersecurity strategy. First of these, is the perspective with which cybersecurity is viewed in an organisation. A technical view of cybersecurity, or strictly limiting it to an IT problem (Kosutic and Pigni, 2020a), considerably restricts its scope and the degree of significance it appreciates. These further effects strategic involvement - such as hiring appropriate personnel at leadership/governance positions equipped to handle this topic - and investment including purchasing appropriate technological equipment and cyber insurance, in it. Understandably, it exposes the organisation to cyber vulnerabilities and potential threats (Boyes, 2015a) to its cyber assets. It has been found that organisations willing to accept cybersecurity as an extension of the risk mandate (Landefeld, Mejia and Handy, 2015), were most optimally positioned to invest in and benefit from robust cybersecurity. Furthermore, interpreting the risk posed by cybersecurity vulnerabilities in its financial equivalent (Nolan, Lawyer, and Dodd, 2019) was found to be a more helpful way to adequately appreciate the business value of cybersecurity, as required by an organisation.

Another aspect within an organisation that emerged as decisive in its stance towards cybersecurity was also its ethical standpoint. Many organisations, erected on the foundation of ethical integrity, were thereby driven to ensure ethical best practices in all their activities, including safeguarding their customer information and providing a secure end-product. Whether within the confines of Corporate Digital Responsibility (Lobschat *et al.*, 2021a) or under their *duty of care* (Lunn, 2014), it could be considered incumbent upon organisations to protect their stakeholders, their information, or any other data. Following ethical principles (Cisco and affiliates, 2023) has increasingly been found to be important for organisations, thereby driving their decisions to safeguard all stakeholder information/data that they seek from them. This involves substantial reliance on robust cybersecurity practices, thus impacting the organisational choice of cybersecurity mechanisms at play.

The final aspect within this sub-theme is the industry sector, which often necessitates the reliance on cybersecurity best practices. Understandably, organisations facilitating financial transactions (like banks (Wright, 2021) and insurance organisations) or organised around financial products and services, have a heightened need for protecting these assets and data. Sometimes, it is also necessitated upon them by the sector's regulatory bodies/authorities. Others, like the technology industry - also, significantly dependent on cyber assets - find themselves requiring robust cybersecurity to safeguard their day-to-day business activities. Yet others, like the public sector - suffering from a lack of inadequate resources (Wessels *et al.*, 2021) to resort to cyber development activities - often have their cyber vulnerabilities exposed through gruesome cyber-crimes. This further reinforces the need for a proactive approach towards cybersecurity, from an organisational perspective.

The next sub-theme is centred around the decision-makers within an organisation, who influence the organisational choices for cybersecurity. One significant aspect of this is the board's level of comfort with cybersecurity; this is often influenced by their own qualifications and past experiences in this field, which further impacts their engagement with associated conversations related to cybersecurity with the leadership and those lower in the hierarchy. Often, it is found that the board members' combined expertise, in matters relating to cybersecurity and its technical elements, is somewhat limited (Gale, Bongiovanni and Slapnicar, 2022). This further exacerbates their inability to be involved in fruitful conversations surrounding various aspects of cybersecurity encompassing concerns, requirements, and potential solutions. While governing boards are increasingly aware of their oversight responsibilities relating to cybersecurity (Hartmann and Carmenate, 2021), the importance of a cyber-aware board (Cerin, 2020) cannot be overemphasised.

The next aspect of this sub-theme is the actual decision-makers of cybersecurity itself, which varies with the organisation. Some organisations are strictly governed by the expertise of the governing board; others are influenced by Audit or Risk sub-committees (Landefeld *et al.*, 2017) which the boards rely on; in other instances, the leadership roles like the CISO (Chief Information Security Officer) (Wessels *et al.*, 2021) play a significant role in these decisions. It has been found that the board members are not always called upon to possess specific expertise in the field of cybersecurity (Nicholls, Kuppa, and Le-Khac, 2021); rather, they are expected to be able to have productive discussions with their executive team within their *duty of oversight* (Landefeld, Mejia and Handy, 2015). Together, they are (Nolan, Lawyer, and

Dodd, 2019) relied upon to make the most organisation-appropriate decisions regarding cybersecurity.

The second theme highlights the array of challenges faced by an organisation, on the path to robust cybersecurity. Interestingly, some of these are surprisingly effective in helping the organisation find clarity in its stance, while others complicate the overall process. The first sub-theme relates to the broad category of cyber-incidents which encompass both the attempts which may or may not lead to an eventual compromise within an organisation. These incidents could be smaller breaches or large-scale attacks, but once they have compromised an organisation's cyber-defences, they have the potential to create considerable financial or legal loss (Nolan, Lawyer, and Dodd, 2019). Whether an organisation suffers from an incident itself or is fortunate to be able to witness it from afar - observing its peers as victims of incidents (Ashraf, 2022) - it is forced into a revaluation of cybersecurity mechanisms. This often leads to a more cyber-aware board, which actively engages in productive conversations (Gale, Bongiovanni and Slapnicar, 2022) around important aspects of organisational cybersecurity. Increasingly, however, more organisations are finding themselves accepting the inevitability of cyber-incidents (Ablon and Libicki, 2015) as a given, and are forced to make adequate pre-emptive preparations for it.

The other aspect is further subdivided into two kinds of challenges, namely: one being macro-economic challenges (like the pandemic which highlighted the need for robust cybersecurity), and the other being industry-level challenges, further complicating the search for appropriate cybersecurity solutions. The Covid-19 pandemic, in particular, has been the cause of an alarming rise in cyber-incidents on account of the overnight shift to remote working, inadequate access to safe internet networks (Pranggono and Arabo, 2021), and lack of physical safeguards to virtual organisational assets (Wirth, 2020). The industry-level challenges are similarly disproportionately impactful for an organisation. These include a host of challenges specific to each industry within which an organisation operates. In some instances, these could include the inability to obtain the necessary personnel exacerbated by a wide skills-gap (Nodeland, Belshaw and Saber, 2019) between what is sought and what is available within the cybersecurity industry. At other times, it is the very nature of technology to rapidly advance - thereby rendering many existing equipment and practices obsolete (Kosutic and Pigni, 2020a). This complicates the process of keeping cyber-assets safe and simultaneously leads to more advanced criminal methods (Bejan, 2022) of breaching the integrity of cyber-assets. The threat is made further sophisticated on account of vast market demand (Ablon and Libicki, 2015) for cyber-criminals due to all the ill-gotten gains derived from their cyber-incidents, which functions as an adept support system for such criminals. These challenges together complicate an organisation's ability to safeguard its cyber defences.

The third theme revolves around the tools often employed by organisations which enabled them to adequately manage their cyber risks. These tools may be categorised primarily into three sub-themes: board engagement levers, insights drawn from past experiences, and the role played by regulation. Board engagement in the context of cybersecurity is often prominent in three valuable ways, the first of which is the appreciation of risk. While most organisations may be understood to engage in cybersecurity decision-making in varying degrees, this study has found that the involvement of the governing board in such conversations has a significant impact on strengthening organisational cybersecurity. A board involved in such conversations can appreciate these risks (Cerin, 2020), thereby prioritising (Nolan, Lawyer, and Dodd, 2019) adequate cybersecurity in the organisation.

Similarly, cybersecurity is often considered an economic cost (Wessels *et al.*, 2021) which inhibits adequate investment required to strengthen it within the organisation. At other times, a lack of clarity on the return from investment in cybersecurity (Barnes, 2019) may also lead organisations to not prioritise it. However, when the governing board can appreciate the business value of the risks associated with cybersecurity and thereby its cost, it acts as a direct lever to enhance the organisational cybersecurity. The third way is enabling the board to lose (or lower) inhibitions as they discuss cybersecurity and make the required decisions. This comes into prominence especially, as board members sometimes lack the necessary confidence (Gale, Bongiovanni and Slapnicar, 2022) to discuss a technical issue, such as this - which does not bode well for the organisation. Furthermore, owing to a potential lack of adequate experience in the field, they may feel discomfort (Landefeld, Mejia and Handy, 2015) in broaching this subject and/or asking the correct questions of leadership required to scrutinise the cybersecurity choices of the organisation. This study highlighted that the boards able to overcome this challenge, posed by such inherent inhibitions, can contribute to robust organisational cybersecurity.

The other sub-theme focusses on insights which organisations can derive from unpleasant past experiences, including cyber incidents. One of these is the importance of correct board language (CBL), which would help the board appreciate the significance of cybersecurity, as necessitated for their respective organisation. This study underscores the importance of finding a common vocabulary which the leadership and board could use to be able to discuss this issue (Cerin, 2020). This would enable the governing board to be able to appreciate the risks and costs and overcome associated inhibitions - which further function as tools for overcoming the cybersecurity-related challenges discussed above.

Another useful insight is to apportion equal importance to people, processes, and technology (PPT), while discussing and deciding cybersecurity issues (Boyes, 2015b). Focussing on any of the three individually would leave the cyber realm of the organisation relatively vulnerable, hence the need to prioritise them in tandem. Hiring the right personnel at all levels (Wright, 2021), along with using and maintaining up-to-date equipment, and incorporating adequate processes (Klinke and Renn, 2006) support organisational cybersecurity mechanisms. The three in tandem work as an optimal defence (Michael *et al.*, 2019) of the organisational cyber realms.

The other insights emerging from the study are a collective of wisdom which organisations have gleaned from their own or others' cybersecurity mishaps. The first among these is the realisation that cyber incidents may be considered inevitable (Ablon and Libicki, 2015), which would enable the organisation to devise the necessary mechanisms to potentially prevent them and protect itself. One another insight highlighted in the study is the significance resilience in cybersecurity governance mechanisms. For a field which is as constantly evolving and dynamic as cybersecurity, the protection measures ought to incorporate a rigorous formulation and continuous adjustment (Sallos *et al.*, 2019) potential. Similarly, prioritising it on the organisational agenda (Hubbard *et al.*, 2021) is yet another insight which, when integrated into organisational strategy, bears fruit for protecting and defending the cyber realm of the organisation.

The fourth theme revolves around the advantages which emanate from an organisation being able to deploy the above tools in confronting the various challenges. These may be primarily categorised into two sub-themes: one of which being a potential competitive advantage, and the other being organisation-specific advantages. The perceived competitive advantage enjoyed by an organisation may be improved through enhanced cybersecurity (Kosutic and Pigni, 2020b). For an issue considered inevitable and with an alarming potential to damage and destroy, proactive measures to ensure robust cybersecurity may be considered a necessary step in deriving competitive advantage. Motivation either by a cyber-aware end customer (Wright,

2021) or the ethics to protect and secure stakeholder data (Michael *et al.*, 2019), are both instrumental in an organisation's decision to employ robust cybersecurity.

The organisation-specific advantages may be appreciated in three ways: enhanced stakeholder trust, upstanding reputation, and business growth. Stakeholders - whether they are customers, employees, or suppliers -all rely on organisations to protect their information and interests (Wirtz *et al.*, 2022), which necessitates transparency (Cisco and affiliates, 2023). Financial organisations are understandably reliant on stakeholder trust (Browdie, 2013) for their well-being, which is contributed to by a robust cyber realm. Thus, a cyber-secure organisation can capitalise on stakeholder trust (De Minville, 2020), thereby leading to other advantages.

One of the evident consequences of stakeholder trust is enhanced organisational reputation, which may only be garnered over the long term. A painstakingly acquired advantage, such as this, has been associated with an otherwise avoidable cyber incident (Gale, Bongiovanni and Slapnicar, 2022), thus of enormous significance to an organisation. While it may be hard to quantify (Aldasoro *et al.*, 2022), an astutely planned and governed cybersecurity mechanism helps the organisation in augmenting its reputation. Similarly, poor cybersecurity has also been associated with poor business performance (Corallo, Lazoi and Lezzi, 2020). Coupled with enhanced stakeholder trust and improved reputation, the organisation can realise growth in business, all emanating from robust cybersecurity measures.

The fifth and final theme emerging from the study highlights the winners as those organisations, which have not only been able to dominate this dynamic and volatile world of cybersecurity concerns but are able to revel in significant advantages, emanating from fortified cybersecurity in the several ways outlined above. Viewing it from the perspective of a thriving organisation in a cyber-reliant future (Abraham and Sims, 2021), choosing a steward-like proactive approach (Ogbanufe, Crossler and Biros, 2021) to cybersecurity, or an ethically-fuelled corporate digital responsibility approach (Wirtz *et al.*, 2022), or incorporating a cyber-resilient system (Hubbard *et al.*, 2021) which relies on the latest technology (Cristea, 2020), are all hallmarks of such a winning organisation. Such an organisation is securely positioned to appreciate all the advantages over its competition, which such a cyber-secure stand allows. In the increasingly competitive yet cyber-vulnerable world of contemporary times, this may be considered a true winning differentiator.

5.3 Emergent Model - Developing Propositions

The results of this study have led to the development of a model which helps explain the association between strategic involvement in cybersecurity and deriving a potential competitive advantage from it. This model is depicted in **Figure 5.1** on the following page.

Securing of cyber assets and the cyber realm is a task which flummoxes many organisations, as there is no one-size-fits all approach to cybersecurity. A combination of factors impacts the choices which lead to decisions with respect to an organisation's cybersecurity mechanisms. This study highlighted the most prominent of these factors as the organisation-specific factors influencing their chosen cybersecurity strategy, coupled with the final decision-makers who craft and implement the said strategy. This study found that the organisation implements this cyber strategy, which considerably impacts its competitive position in the industry.

At this stage, it is important to note that certain propositions (P1b and P11) have emerged within the model demonstrating what may be construed as reverse causation. This is acknowledgement of the impact of certain factors/ processes in influencing other outcomes/ processes in both linear and non-linear ways. Furthermore, this allows for perpetuating the loop and a continuous influence on outcomes.

However, on the path to achieving robust cybersecurity, the organisation invariably encounters several challenges which eventually determine how cyber-secure its future is. This realisation brings to the fore the following proposition:

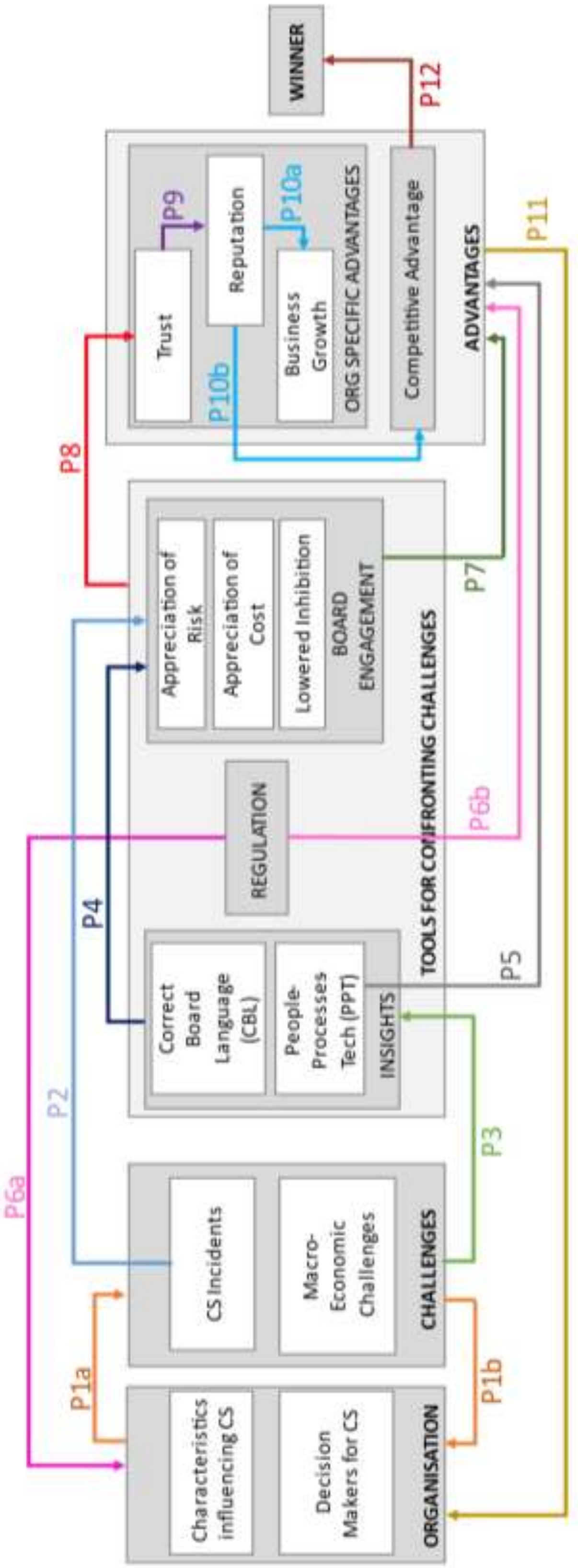

Figure 5.1 Emergent model from the study. ***Source****: Developed by the author.*

P1a: An organisation faces challenges on the path to robust cybersecurity.

Consequent to an organisation crafting its cyber-strategy, it faces obstacles in implementation. Several factors threaten to expose its vulnerabilities and weaken its competitive position, thus complicating the path to robust cybersecurity. These could be posed through cybersecurity incidents faced by the organisation, or other macro-economic challenges which may impact its competitors as well. While it may seem that both these kinds of challenges are outside the scope of the organisation, the organisation itself differentiates itself from others in the way it chooses to overcome and/ or respond to these challenges. The following proposition may thus be formulated:

P1b: The challenges faced by an organisation impact its future cybersecurity-related decisions.

As we realise that the organisation's chosen response to the above challenges helps differentiate itself from others, it would follow that these challenges are instrumental in the organisation and all its cybersecurity decisions. Whether an organisation suffers considerably or not at all, whether it chooses to alter its existing cyber-strategy or not, whether the challenge has affected its future choices in other functions or not; all of these are deliberate choices which shall govern its cyber-future. All future decisions related to cybersecurity strategy, implementation, and organisational welfare hinge on the organisational response to these challenges that the organisation found itself forced to interface with.

This study found that, in most cases, organisations faced with cyber incidents (either their own or those of their peers) choose to recalibrate their existing cyber-strategy. This includes decisions related to the personnel (whether they need to hire internal or external resources to manage it, considering the level of importance afforded to cybersecurity), board-agenda item (or departmental choice of the IT department), financial investments for cybersecurity, processes associated with cybersecurity governance or management, and even the level of transparency the organisation chooses to maintain with its stakeholders who have suffered an incident. All these strategic choices impact the vulnerability of its cyber realm in the future. A proactive stance helps strengthen its cybersecurity, while a lackadaisical approach renders it potentially more vulnerable (as it is now exposed to potential future cyber criminals as well).

The proactive and positive response to these cyber incidents has revealed an insightful learning from the study. This learning leads to the following proposition:

P2: Cybersecurity incidents precipitate board engagement in cybersecurity discussions.

Regardless of the kind and intensity of a cybersecurity incident, it often facilitates discussion of cybersecurity matters at a board level. Whether it was a small incident which did not lead to a considerable expense or led to a breach, or was purely experienced as a peer, an organisation finds itself attempting to prevent future cyber-related vulnerabilities. Since the matter of cybersecurity has now achieved a priority, it leads to the involvement from the highest echelon of the organisation. Board members engage cybersecurity discussions in either seeking answers from their executive and/or scrutinising executives' decisions related to cybersecurity. In either case, cybersecurity garners board engagement and priority.

This is realised through three crucial ways, the first of which is a board henceforth capable of appreciating all the risks accruing from loss or compromise of their cyber assets. The ability to associate a business value to cyber risks is a significant step towards making appropriate decisions in strengthening cybersecurity. The second one, similarly, is appreciating the cost of cybersecurity, with respect to the level of investment it necessitates, instead of being merely considered as a cost centre to the organisation. Being able to apportion adequate budgets for taking a proactive stance towards robust cybersecurity is another outcome of board engagement. The third way is the board overcoming their inhibitions associated with the perceived technical nature of cybersecurity to engage in a forthright discussion with their executive.

This proposition also brings to fore the realisation that the challenges an organisation is forced to confront also present opportunities to learn from and prevent future occurrences of a similar nature. From this, the next proposition emerges:

P3: Challenges faced by an organisation facilitate the discovery of invaluable insights.

Through all experiences - pleasant or otherwise - an organisation learns valuable lessons which help in strengthening its position in preventing future re-occurrences of cyber-incidents. Gleaning insights from past challenges and employing them to overcome future challenges is vital for organisational success. These valuable insights are crucial to withstanding incidents, both in the cyber realm and those at a larger scale, beyond the immediate control of the organisation. The first among these is the importance of using an appropriate language in the boardroom, which would enable engagement from the board. The second is the significance of deploying cybersecurity in tandem with its most crucial elements - people, processes, technology.

The first insight paves the way for the next proposition:

P4: Appropriate articulation of cybersecurity concerns in the boardroom enables board engagement.

Many instances of cybersecurity challenges faced by an organisation are on account of a misaligned discussion on cybersecurity between the board and the executive. This may be consolidated to the lack of a common lexicon employed between the board and its executive, which conveys the risks and costs of cybersecurity with commensurate importance while allowing an uninhibited discussion from both sides. Thus, using the correct board language with respect to cybersecurity is an important lesson.

Despite limited experience with cybersecurity events (or limited experience with the technical aspects associated with the field), the ability to have sound discussions is vital in order to be able to engage in the topic. A governing board capable of appreciating the risks, costs, and gravity of the cybersecurity concerns and vocabulary is most prudently positioned to craft and scrutinise a cybersecurity strategy with its executives, which is optimal for the organisation. The other insight similarly enables the organisation to derive advantages, which leads to the next proposition:

P5: A balance between the people, processes, technology involved in cybersecurity leads to organisational gains.

The principle of People, Processes, and Technology has been around for many decades; yet its inclusion in cybersecurity strategy, though equally important, is relatively new. It highlights the significance of maintaining a balance of priority between these three elements while crafting a cybersecurity strategy. Prioritising one over the other may lead to an imbalance, which would invariably lead to exposed cyber vulnerabilities. Hiring appropriate people, delineating adequate processes, and utilising the most effective technology simultaneously are key to a robust cybersecurity mechanism.

Cybersecurity incidents are perceived to be caused primarily owing to human error, which may be minimised by adopting strategies to train the personnel to recognise potential cyber-threats and thus prevent them. Similarly, implementing processes including incident-response plans - in cases of cyber incidents/contingencies - may reduce response time and allow the system to resume function without the need for human involvement. Furthermore, incorporating the latest technologies for the implementation of the said cyber strategy may enable the organisation to derive advantages pertaining to incidents prevented and losses averted.

While these may seem simplistic, in contemporary times, organisations which are able to experience such gains easily outperform their peers who are struggling to keep their cyber realms secure and assets uncompromised. These organisations, therefore, gain stakeholder trust, which may be further leveraged to enhance organisational reputation, thereby leading to business growth and other advantages.

In certain instances, organisations are obligated to secure their cyber realms owing to strict regulations. The next two propositions emerge, which highlight the wide-ranging impact regulations may be considered to have:

P6a: Regulations impact each organisation in a unique way.

Regulations requiring organisations to follow certain cybersecurity practices - whether it involves following preventative measures or highlights incident-response mechanisms - allow no accommodation for an organisation’s individual choice. However, depending on geographical borders, such regulations vary depending on the industry sector an organisation functions in. For instance, the banking and financial services sector is stringent in implementing the above-mentioned security expectations from organisations within the industry. Failing to do so leads to substantial penalties and legal costs, which function as a lack of positive reinforcement for organisations to follow suit.

However, others outside the financial services sector may not be governed by the same expectations, which allows them certain scope to decide upon their cybersecurity stance. Similarly, the involvement of the board, specific committees assigned to govern cybersecurity concerns and department decision-making associated with cybersecurity strategy and implementation, are other factors thus impacted by regulations or their lack thereof. This further underscores the positive impact regulations can have on organisations, which are compelled to adhere to strict regulatory requirements within their cybersecurity mechanisms, thus highlighting the next proposition:

P6b: Regulations create opportunities for organisations.

For all those organisations which are bound to follow regulatory procedures or practices leading to the formulation or influence of their cybersecurity strategy, the outcome invariably strengthens their cybersecurity stance. Whether it is to safeguard stakeholder interests or prevent a cascading impact on other organisations/industries linked with such an organisation, following regulations - voluntarily or not - protects the cyber realm of such organisations, thereby enabling certain advantages.

Such organisations, on account of their protected cyber-assets, can either prevent most cyber-breaches or are able to resume function with the least losses/inconvenience. This enables trust from their different stakeholders for having protected their interests and information, and also performed the duty of care. This trust further leads to an enhanced reputation within the industry, which understandably is strengthened - thereby enhancing their business prospects.

The third tool employed to confront challenges is board engagement, which similarly allows organisation-specific advantages to be derived. The next proposition thus emerges:

P7: Board engagement in cybersecurity discussions facilitates cybersecurity-led advantages.

A governing board capable of discussing cybersecurity issues without inhibitions, as well as a commensurate appreciation for the potential risks and costs, which may be incurred following a cyber incident, is able to have fruitful discussions of cybersecurity with its executive. Such an engaged board thus appreciates the appropriate priority necessitated by cybersecurity and takes the necessary decisions to safeguard the organisational cyber realm, which protects stakeholder interests. This protection further generates stakeholder trust, enabling the organisation to enhance its reputation, and derive associated advantages. The next proposition follows as an outcome of this, and other tools employed by the organisation to confront challenges:

P8: The tools an organisation employs to confront challenges enhance stakeholder trust.

The previous propositions highlighted a combination of three tools which organisations choose to employ, to overcome the challenges caused by cyber incidents and other challenges beyond their control. These tools - in the form of insights gleaned from past experiences, board engagement in cybersecurity discussions, and regulatory requirements - strengthen the organisational cyber realm. With their cyber assets - which often include stakeholder information, financial records, and intellectual property - protected, the organisation gains trust from its stakeholder. The next proposition emerges:

P9: Stakeholder trust strengthens organisational reputation.

Stakeholder trust is instrumental in leveraging enhanced organisational reputation and other advantages. Cyber incidents lead to a compromise of cyber information, and organisations unable to protect their stakeholder interests in the cyber realm, thus suffer from considerable impact to their reputation. Considering the alarming frequency of such events, the organisations which can safeguard their stakeholder interests are especially able to gain enhanced reputation within the industry. This reputation is of particular significance as it leads to other substantial benefits for the organisation, besides being otherwise unattainable in the short term.

The next two propositions follow, which underscore the significance of an upstanding organisational reputation.

P10a: Good organisational reputation helps in business growth.

An enhanced organisational reputation is understandably the business objective of most operational organisations. For those functioning with the profit motive, it is especially vital towards gaining business growth, as it attracts additional stakeholders to be associated with the organisation.

P10b: Enhanced organisational reputation facilitates competitive advantage.

An organisation capable of upholding stakeholder interests gains their trust, which it can then leverage to enhance its reputation. This reputation, in turn, can facilitate a competitive advantage for the organisation which it has secured through securing its cyber realms. Thus, the path to robust cybersecurity through a proactive stance helps an organisation in building a reputation which enables an advantage that several of its competitors are unable to experience. In contemporary times, when the infamy of cybersecurity incidents is widespread, those rare organisations capable of preventing them and upholding reputation gain a competitive edge, besides expansion of business prospects.

In such cases, these organisations are persuaded to continue their proactive stance towards robust cybersecurity, in order to sustain those advantages. This brings to the fore the following proposition:

P11: Organisational advantages impact the organisation's future decisions for cybersecurity.

An organisation which is experiencing a host of advantages - including stakeholder trust, enhanced reputation, and business growth owing to robust cybersecurity mechanisms - is then able to view cybersecurity in an encouraging context. It thus determines its future actions pertaining to the formulation and implementation of cybersecurity strategy. Whether it was compelled to follow regulations or had gleaned insights from past experiences, or even had steward-like board members being proactive towards robust cybersecurity, once it experiences the said advantages, it maintains a similar stance. A consistent proactive approach to robust cybersecurity thus enables the sustainability of the advantages accruing from it, which highlights the next proposition:

P12: Cybersecurity-enabled competitive advantage results in organisational success (winner).

An organisation with robust cybersecurity can uphold stakeholder trust, which leads to reputational gain, and expansion of business, thus enabling an advantage over its competitors. This rare combination of advantages, enabled from a proactive cybersecurity stance, may be considered the cyber equivalent of the *elixir of life*, which allows an organisation to not only survive in an increasingly volatile scenario but also thrive when a significant majority of its peers is unable to. This study emphasises the experiences of practitioners who have either sought this exceptional winner status or have found it and are able to reveal their insights.

It is imperative to recognise that robust cybersecurity is greater than a mere combination of the sum of various aspects of proactive cybersecurity mechanisms. It underscores a winning combination of optimally apportioned elements, which are subjective to each organisation. However, a proactive cybersecurity stance may be considered the origination of a journey which has the potential to help the organisation reach a winning status.

5.4 Evaluation of Research Quality

As may be considered widely acknowledged, qualitative research - and with it the qualitative inquiries - need to demonstrate the credibility of their studies (Creswell and Miller, 2000). However, even within the scope of studies in general - whether quantitative or qualitative - the evaluation of the studies serves an important purpose with respect to ensuring the validity and applicability of the findings. Thus, scholars often question the rigour, authenticity, and trustworthiness (Lincoln and Guba, 2007) of studies.

This research has been meticulous through the entire process to ensure that the exploration of this topic has been conducted with diligence. A number of factors highlighted by scholars to evaluate the trustworthiness (Lincoln and Guba, 2007) is maintained. The following table outlines the main criteria against which the trustworthiness and validity of this research may be weighed.

*Table 5.1 Evaluation of research quality. **Source**: Compiled by the author*

Evaluation Criteria	**Hallmarks of Criterion**	**Operationalisation of Criteria in this study**
Credibility	Keeping interpretations authentic and accurate to interviewee descriptions (Drisko, 1997)	Remained aware of the impact of research procedures on credibility (Lietz and Zayas, 2010) and of the revealed truth external to researcher experience (Thorne, 1997)
	Managing researcher bias (Padgett, 2008)	Built and engaged in reflexivity regarding personal influence through dialogue with supervisors and peers, participated in other research projects throughout the entire research process (Guillemin and Gillam, 2004)
	Using data triangulation (Padgett, 2008)	Gathered data through multiple sources - different participants from different sides of the table, to enable completeness (Drisko, 1997) of response to the research question
	Ensuring research decisions are consistent with the researcher's intended purpose (Patton, 2002)	Hence, the comprehensive chapter on research methodology with a focus on research design, enquiry logic and other procedures
	Member-checking (Creswell and Miller, 2000; Padgett, 2008)	Sought feedback on the findings from a few of the participants. (Shenton, 2004) to increase the trustworthiness of research (Lincoln and Guba, 2007)

Transferability	Ensuring the context is described in detail and relates to the context of other groups and settings (Devers, 1999)	Sought participants from a variety of backgrounds and industry sectors to increase the probability of transferability of findings. Moreover, used the applicability of findings in other backgrounds and settings of organisations with varying firm sizes, the sizes of governing boards, etc.
	Maintaining the research's credibility is important to contribute to the knowledge base (Lietz and Zayas, 2010)	Considered and implemented many factors to ensure the credibility of the research procedures.
	Clearly describing research methods and findings to aid the check on validity by others. (Lewi and Ritchie, 2003)	Chapter 3 clearly described the philosophical choices, methods used, and processes involved in analysing data, with 'transparency' and 'thick description' (Lincoln and Guba, 2007), allowing others to verify transferability to other settings (Lewi and Ritchie, 2003).
Auditability	Maintaining an audit trail (Lietz and Zayas, 2010; Holloway and Wheeler, 1996)	Demonstrated an iterative process that changes as the study unfolds (Drisko, 1997; Devers and Frankel, 2000; Davies and Dodd, 2002; Morrow, 2007) –initially involving the interview of only board directors, but later also including executives, to provide triangulation of data. The sample size could reach 35 but ended at 31 as saturation was reached.
	Engaging in peer debriefing (Padgett, 2008)	Had multiple discussions with supervisors and other colleagues from the field to discuss research decisions and procedures and gain important feedback, which would enhance the quality of the project (Shenton, 2004)

Confirmability	Seeking diverse experiences (Drisko, 1997) to achieve exhaustive exploration of the research subject.	Disconfirmed evidence (Creswell and Miller, 2000) provides further support of the account's credibility, while it does not outweigh the confirming evidence. This is because reality is multiple and complex.
	Demonstrating findings and data as clearly linked (Lietz and Zayas, 2010)	Maintained member-checking, peer debriefing and audit trails through the course of the study

This exploration into understanding how strategic decision-makers in organisations incorporated cybersecurity in their corporate strategy, has relied on several practices to ensure the credibility, transferability, auditability, and confirmability criteria have been met.

The methodology is justified from a philosophical standpoint of constructivist ontology and interpretivist epistemology, which guide the further choices with respect to research design, enquiry logic, and other methodological decisions. Elucidating these decisions in Chapter 3 was a key step toward fulfilling the trustworthiness criteria. To ensure credibility, the study has leaned on strategies such as data triangulation (Padgett, 2008) and member-checking (Creswell and Miller, 2000), among others, outlined in the adjacent table.

Similarly, comprehensive detailing of the methodological choices, along with maintaining an applicability with other groups and settings (Devers, 1999), have been key in ensuring the transferability of the findings. The auditability criterion has been achieved through the employment of strategies such as peer debriefing (Padgett, 2008) and maintaining an audit trail (Lietz and Zayas, 2010). To ensure confirmability of the findings, the study sought to collect diverse experiences (Drisko, 1997), which would enable a realistic account of the exhaustive exploration conducted for this research.

The next section reiterates the research aim and objectives of this study, in addition to elucidating accounts of justifying whether they have been or not.

5.5 Achievement of Research Aims and Objectives

This section both reiterates the aims and objectives which this research intended to fulfil and discusses the nature and extent to which they have finally been achieved. Furthermore, the following table summarises the research objectives and key findings from the study.

Table 5.2 Summary of objectives and findings. ***Source****: Developed by the author.*

S. No.	Research Objectives of Study	Key findings identified through sub-themes	Relationship between research objectives and findings
1	To explore the extant literature surrounding strategic decision-making on cybersecurity strategy, with potential possibility to derive competitive advantage from it.	Organisational characteristics impacting CS needs	This research objective has been met as the research examined organisations, their decision makers crafting and implementing strategy, and external factors impacting cybersecurity strategy.
		Organisational decision makers for CS	
		CS Incidents	
		Macro-economic Challenges	
2	To ascertain precisely how board directors, in conjunction with their executives, craft their cybersecurity strategy through elite interviews with 25-30 such individuals.	Board Engagement Levers	This research objective has also been achieved as the study conducted an in-depth data collection through 31 interviews, ascertaining the key levers which enable board engagement, in addition to unearthing insights and the impact of regulation on devising a robust cybersecurity strategy.
		Insights	
		Regulation	
3	To propose a model explaining the challenges which consequently determine an organisational stance on cybersecurity strategy and implementation, and the path to realising competitive advantage from it.	Competitive Advantage	This objective has been achieved through a model which delineates the path to deriving organisational advantages through robust cybersecurity, including competitive advantage.
		Organisation Specific Advantages	
		Winners	

The following section reiterates the research aims and objectives and explains the ways in which each of those has been achieved within the context of this study.

Research Aim: **To investigate the way governing boards, in association with their leadership team, incorporate cybersecurity as a critical element of their corporate strategy in order to realise a competitive advantage.**

Considering this, the study has been able to comprehensively understand how, as part of the larger strategy, cybersecurity mechanisms are strategically prepared for. Additionally, this study also discovered the priority habitually conferred upon cybersecurity decisions, including the key decision-makers for the task, as well as the impact of those decisions on the organisational future and welfare. While the task required gaining an in-depth understanding within the premise of evolving digitalisation and increasingly exposed organisational cyber realms, the study has been successful in uncovering the significant impact of strategic involvement in cybersecurity decision-making. This occurrence is referred to as cybersecurity governance, which incorporates a strategic intent and an enhanced approach over mere cybersecurity management (which is primarily an operational mechanism).

Research Objective 1: **To explore the extant literature surrounding strategic decision-making on cybersecurity strategy, with potential possibility to derive competitive advantage from it.**

The literature centred around organisational cybersecurity stance, related decision-making at the board and executive levels, and strategic choices - with respect to deriving a competitive advantage - has been diverse and dynamic. Especially owing to an ever-evolving field of technology, which has a considerable influence on cybersecurity practices, literature is relatively underdeveloped. While the academic research has comprehensively explored potential sources of competitive advantage, the sources have yet not been associated with cybersecurity strategies. However, this link has been successfully investigated through this study.

Also, with respect to decision-making at an organisational level, literature has been split into two schools of thought - one which placed it purely within the scope of the governing board, and the other which did so in the hands of the executive. However, in an operationally intensive yet technically scrupulous domain, (which has not traditionally been the scope of governing board), cybersecurity was discovered to be on a joint agenda with both the boards and executives playing key roles in tandem. Thus, despite being a developing field of examination, this research objective has been met by this study.

Research Objective 2: **To ascertain precisely how board directors, in conjunction with their executives, craft their cybersecurity strategy through elite interviews with 25-30 such individuals.**

Through an inductive enquiry logic, this research embarked upon interviewing at least 25 governing board and executive team members with access to and knowledge of the intricate processes involved in crafting and implementing organisational cybersecurity strategy. Moreover, this study was able to interview 31 such individuals to gather an acute understanding of the delineation of role and responsibilities between the governing board and their executives, while making decisions for organisational cybersecurity. The study observed that while the decisions surrounding the crafting of cybersecurity strategy is within the board purview, it is conducted in close association with the executives to elevate opportunities of operational success in its implementation. Furthermore, the findings revealed a strong association between strategic involvement in cybersecurity decision-making and the potential to derive competitive advantage from it. Thus, this research objective was also achieved.

Research Objective 3: **To propose a model explaining the challenges which consequently determine an organisational stance on cybersecurity strategy and implementation, and the path to realising competitive advantage from it.**

This final objective relates to explaining the context of cybersecurity decision-making in an organisation with a specific perspective on the board-executive role, with the potential to derive competitive advantage from it. A model demonstrating the link between these two elements has been arrived at, which explains the surprising, yet realistic steps involved in deriving advantages from robust cybersecurity in an organisation. It outlines the importance of prioritising the protection of shareholder information within the cyber realm of an organisation. Through this the organisation can gain stakeholder trust, which it can then leverage to enhance organisational reputation, which has long-term advantages. One of these is specifically having an advantage over an organisation's competitors, which allows it to differentiate itself, thereby enabling success. This objective has been met.

Thus, with the achievement of aims and objectives of this study, this research demonstrates the potentially beneficial association between strategic involvement in cybersecurity decision-making and organisational success consequent to it, which has important connotations to both research and praxis.

5.6 Contributions to Knowledge

This study supports seminal literature in exemplifying, extending, confirming, and advancing certain concepts found there. Resource-Based View (Wernerfelt, 1984) being the foundation for this study, has immediate contributions with respect to recognising cybersecurity as an extension of the IT asset of an organisation which, when fortified, has the potential to enhance its reputation - thereby providing competitive advantage. This aspect has implications for both extant literature and practitioner reports, thus making contributions to academic research as well as industry practice in the near future. These are elucidated in this section.

5.6.1 Contributions to Theory

This research makes contributions to the field of strategic management literature with implications for Resource-Based View (Wernerfelt, 1984) and Dynamic Capabilities (Teece, Pisano and Shuen, 1997), which have been detailed as follows:

5.6.1.1 Contribution to Resource-Based View

Resource-based View (Wernerfelt, 1984) or the Resource-based Theory (Barney and Clark, 2007) has been the foundation for this study, with its focus on the resources of a firm which allow it to gain and sustain superior performance (Barney and Clark, 2007). This study thus works to contribute to these seminal works in the field of strategic management. The primary contributions are highlighted in **Table 5.3** below:

*Table 5.3 Contribution to Resource-Based View. **Source**: Developed by the author.*

Theory/research	Contribution	Extent of Contribution
Resource-Based Theory (Mata, Fuerst, Barney, 1995)	Robust cybersecurity is an integral component of an organisation's cumulative IT assets.	**Confirms** and **extends** the IT-enabled competitive advantage argument, by incorporating cybersecurity as a legitimate IT manifestation. **Illustrates** its relevance through empirical tests.
Resource-Based View (Wernerfelt, 1984)	Robust cybersecurity enhances reputation, which enables competitive advantage.	**Confirms** and **extends** the notion of reputation as an intangible asset in the context of attaining competitive advantage.

Resource-Based View (Wernerfelt, 1984)	Deriving competitive advantage from reputation through robust cybersecurity advances the perspective on resources and expands it to include stakeholder trust.	Incorporating cybersecurity mechanisms in the information era **advances** the application of the RBV view in that it enhances the notion of the resource in question. Stakeholder trust may not yet have been viewed as a resource from which to leverage reputation.

Contribution 1 - Robust cybersecurity is an integral component of an organisation's cumulative IT assets.

The notion of deriving competitive advantage from an IT has been accepted as having initially been propounded (Barney, 1991) a few decades prior. This study confirms and extends the IT-enabled competitive advantage argument by incorporating cybersecurity as a legitimate IT manifestation. This research also illustrates the relevance of this concept through empirical tests. Literature has pointed out the significance of incorporating IT as an integral element of their corporate strategy, which leads to deriving a superior performance from it. As pointed out by Mata, Fuerst and Barney (1995), the potential for competitive advantage is derived from organising and managing more than aspects of IT itself. The aspects of IT have also been outlined as - customer switching costs, access to capital, proprietary technology, technical IT skills, and managerial IT skills (Mata, Fuerst and Barney, 1995).

As evidenced by this study, the way an organisation can strategise cybersecurity to safeguards its stakeholder data allows it to leverage stakeholder trust, thereby enhancing its reputation and allowing competitive advantage. Robust cybersecurity mechanisms have been known to incorporate a strategic involvement - hiring the appropriate personnel at all levels, investing in latest technology and equipment, purchasing necessary cybersecurity insurance, and undertaking cybersecurity certifications. The precise combination of these elements allows the differentiation one organisation can experience through its planning and management/governance of cybersecurity as an aspect of IT.

Furthermore, it is useful to note that literature has highlighted the tendency of organisations to define themselves in terms of the technology (Wernerfelt, 1984) they adopt. This is advanced through this study by exemplifying that the specific combination of cybersecurity decisions, and the choices made, is subjective to each organisation. This combination allows them varied degrees of success in their cybersecurity journey and, ultimately, in acquiring robust cybersecurity. Thus, this study confirms and illustrates this aspect of firms to internalise their technological behaviour, which eventually impacts their success in protecting their cyber realm.

Contribution 2 - Robust cybersecurity enhances organisational reputation, which enables competitive advantage.

The findings from this study propose the significance of safeguarding stakeholder data, thereby leveraging their trust leading to enhanced reputation, and deriving competitive advantage from it. Accepting the notion that reputation can only be built over a long period of time (Mata, Fuerst and Barney, 1995), this study confirms and extends this notion of reputation as being an intangible asset (Prahalad and Hamel, 1990) and invisible asset (Itami, 1987), from the context of attaining competitive advantage.

Moreover, honourable reputation (Klein, 1978) and trustworthiness (Barney and Zajac, 1994) have been accepted as socially complex, intangible assets (Rindova, Williamson and Petkova, 2010). Hence, once acquired, reputation may not be imitated as it has been cultivated through a complex process subjective to each organisation - as pointed out earlier - which causes causal ambiguity (Mata, Fuerst and Barney, 1995). This subjective mechanism consists of a large number of small decisions and tacit attributes (Reed and DeFillipi, 1990) to strengthen cybersecurity to safeguard stakeholder data, further earning their trust. This study highlights, reinforces and confirms this view of reputation and trust as intangible assets, which have been laboriously earned and allow the organisation to derive competitive advantage from them.

Contribution 3 - Deriving competitive advantage from reputation through robust cybersecurity advances the perspective on resources and expands it to include stakeholder trust.

Resources with the potential to contribute to long-term competitive advantage may yet have not included stakeholder trust by safeguarding stakeholder information. Thus, incorporating robust cybersecurity mechanisms to protect stakeholder information, especially in the information era, enhances and expands the notion of the resource in question. Building on the argument of protecting stakeholder information - which allows stakeholder trust - forms the foundation of this study which highlights this cybersecurity-enabled competitive advantage.

This has been underscored in literature, highlighting the ability of an organisation to respond to customer needs effectively and efficiently, thereby allowing a potential competitive advantage (Barney and Clark, 2007). Furthermore, in the context of a digitalised 4.0 economy which may be recognised as an example of dynamic environmental conditions (Peteraf and Bergen, 2003), the importance of orienting to customer needs is magnified as much as it entails protecting their information within the organisation. This advances the theoretical feedback loop by expanding the scope of resources to include trust that an organisation has earned from its stakeholders.

5.6.1.2 Contribution to Dynamic Capabilities

Inherently, the dynamic capabilities approach relies on exploiting internal and external firm-specific competencies to address changing environments (Teece, Pisano and Shuen, 1997). In this context, this study contributes to the theoretical discourse by augmenting the notion of dynamic capability to include a robust cybersecurity mechanism, which may enhance the organisation's ability to fend off attacks exposing its cyber vulnerabilities. The contributions to this theory are briefly highlighted below in the **Table 5.4**.

Table 5.4 Contribution to Dynamic Capabilities View. ***Source****: Developed by the author.*

Theory/research	**Contribution**	**Extent of Contribution**
Dynamic Capabilities (Teece et al, 1997)	Robust cybersecurity enhances reputation, which enables competitive advantage.	**Illustrates** the use of mechanisms which ensure robust cybersecurity as a dynamic capability that leverages stakeholder trust to enhance organisational reputation.
Dynamic Capabilities (Teece et al, 1997)	In environments of rapid technological change, upholding stakeholder trust (by safeguarding stakeholder information) is key towards deriving a competitive advantage.	**Confirms** and **extends** the notion of competitive advantage through assets and the utilisation of these assets in a changing market - by safeguarding stakeholder information through the deployment of mechanisms which ensure robust cybersecurity.

Contribution 1 - Robust cybersecurity enhances organisational reputation, which enables competitive advantage.

In the context of IT as a dynamic capability, which has been explored in extant literature, this study helps advance the notion of IT to include cybersecurity as a dynamic capability. This capability which thus far has primarily been construed in a supporting operational role, may - through this study - be now reconceptualised in the context of a strategic role. In many instances, the utilisation of robust cybersecurity mechanisms is an outcome of crisis-ridden or otherwise challenging external environment factors, such as the Covid-19 pandemic and the associated lockdown, which forced many organisations to adopt remote working routines.

Certain scholars view such developments as *ad hoc problem-solving* (Winter, 2003) approaches, rather than capabilities which may enable competitive advantage in the potential future. Clearly, as an operational choice, cybersecurity mechanisms - however robust - may not enable an organisation to derive an advantage over all its competition. However, strategically exploiting cybersecurity in context of the *menu of different technological choices* (Teece, Pisano and Shuen, 1997) available to each organisation allows cybersecurity the potential of a dynamic capability. Makadok's (2001) view that organisational capabilities are firm-specific and embedded in its processes is illustrated when incorporating its proactive strategic cybersecurity choices.

Contribution 2 - In environments of rapid technological change, upholding stakeholder trust (by safeguarding stakeholder information) is key towards deriving a competitive advantage.

This study thus confirms and extends the notion of competitive advantage by recognising the protection of stakeholder information as an elementary stakeholder (customer) need, which allows it to capitalise on their trust, thereby garnering enhanced reputation. Thus, this research confirms the utilisation of the asset of stakeholder trust, which is derived from protecting stakeholder information, through the deployment of robust cybersecurity practices. These practices, furthermore, are a specific set of capabilities which have been honed over time through positive and negative experiences and thus cannot be merely purchased; they are developed or built (Teece, Pisano and Shuen, 1997) in an organisation.

As pointed out by Eisenhardt and Martin (2000), even the small failures of the organisation provide great motivation to learn from them and enhance future processes. In the context of cyber incidents, minor events in an organisational past serve as adequate experiences to recalibrate a strengthened cybersecurity mechanism that can protect its invaluable asset, which is the stakeholder trust. Rather than simply purchasing the combination of elements needed to secure the stakeholder information, these specific element choices are driven through internal processes and developed over time, thus being extremely specific to each organisation. This study empirically confirms this view of robust cybersecurity as a dynamic capability from which competitive advantage can be potentially derived.

The next subsection elucidates the contribution this thesis makes to the field of practice, especially the top of the corporate pyramid and its strategic decision-makers, and to further influence the practitioners and organisations themselves.

5.6.2 Contribution to Practice

This thesis has investigated the evolving world of safeguarding organisational cyber realms, thereby potentially improving their ability to earn advantages over their competitors through board involvement. The framework arrived at has useful connotations for organisations and the way they approach the area of cybersecurity, and craft decisions for it, thereby being *problem-driven* (Corley and Gioia, 2011) as highlighted by scholars. This led to the realisation that the strategic perspective to cybersecurity governance has an impact on the organisational reputation, success, and competitiveness within the industry, far beyond the inherent safeguarding of their cyber assets. Following are the primary contributions of this research for the field of organisational practice, highlighted in **Table 5.4**.

Table 5.5 Contribution to practice. ***Source****: Developed by the author.*

Type of Contribution	**Contribution**
Degree of impact	Linking the cybersecurity and organisational reputation to competitive advantage is a novel perspective, which aids the organisational motivation to devote strategic focus towards operationalising cybersecurity.
Scope of influence	Research such as this is useful for organisational practice, besides having potential policy implications, which currently vary by geography and leave much to be desired.
Nature of offered remedies	Offers practical solutions and a fresh perspective to cybersecurity governance, which creates a high likelihood

	for organisations to derive several advantages from it, over their competition.
Relevance and pertinence of study	In the 4.0 economy, with increasing reliance on a digitalised world, the potential for damage and/or demise from cybersecurity failures is high and rather under-researched, which this study aims to resolve.

Contribution 1 - Linking the cybersecurity and organisational reputation to competitive advantage is a novel perspective, which aids the organisational motivation to devote strategic focus towards operationalising cybersecurity.

Extant literature, coupled with organisational practices, bear witness to prioritising cybersecurity at a departmental level, which lends itself to operational policies thus far. Identifying the link between strategic decision-maker involvement in corporate strategy for cybersecurity practices and potentially deriving competitive advantage from it, allows new avenues for the discussion of competitive advantages. As highlighted by this study, when an organisation can identify the potential of this relationship, it enables the decision-makers to enact cybersecurity governance over its management.

The best practices involved in safeguarding stakeholder information to leverage their trust, earns the organisation an upstanding reputation, which further enables competitive advantage. This association is novel and offers perspectives which allow organisations to enhance their cybersecurity mechanisms. Strategic involvement in cybersecurity decision-making has the potential to offer the organisation long-term advantages, and this study presents useful lessons from that perspective.

Contribution 2 - Research such as this is useful for organisational practice, besides having potential policy implications, which currently vary by geography and leave much to be desired.

While this study offers original perspectives on improving cybersecurity mechanisms, thus allowing advantages over competition, it simultaneously has vital policy implications. Firstly, the cyber realm is challenging to govern as it is not defined by geographical jurisdictions. Furthermore, as it is an ever-evolving realm, being able to craft policy regulations apropos to the current requirements is an onerous task. Finally, since policies are significantly influenced by organisational practices, learning the potential impact to them is beneficial to guide future pertinent regulations. This study thus provides effective opportunities to further explore the links described here, which may enable more suitable policies capable of safeguarding the larger cyber realm.

Contribution 3 - Offers practical solutions and a fresh perspective to cybersecurity governance, which creates a high likelihood for organisations to derive several advantages from it, over their competition.

Through this research, the limitations of engaging in cybersecurity management have been highlighted, besides extolling the virtues of cybersecurity governance. Thus, this study is valuable in offering remedies to the limitations of inadequate strategic attention yielded to cybersecurity. With the aim of safeguarding stakeholder information, preventing hostile cyber incidents, upholding organisational reputation and financial stability, the strategic decision-makers may advance the organisational welfare and fortune through robust cybersecurity. By identifying the significance of governing cybersecurity strategy and implementation, the organisation may then take further steps to safeguard its cyber assets. Thus, this study emphasises the need to move beyond cybersecurity management and elucidates the merits of cybersecurity governance.

Contribution 4 - In the 4.0 economy, with increasing reliance on a digitalised world, the potential for damage and/or demise from cybersecurity failures is high and relatively under-researched, which this study aims to resolve.

This research is especially valuable at this stage of technological evolution characterised by 4.0 economy and organisational reliance on digitalisation, which is increasingly exposing cyber vulnerabilities of organisational cyber realms. Owing to the relatively new influence of this evolution stage, this field could benefit from research such as this which offers timely and pertinent solutions, besides highlighting directions for future investigations in this field, aligning with the view of orienting toward prescience to increase utility (Corley and Gioia, 2011) in the practitioner community. By pointing out the current practice, in addition to offering new perspectives of viewing the challenges, this research enables an opportunity to not only be cyber-secure but also derive organisational advantages from it. In an era where cyberspace has been recognised as the fifth operational domain (Ross and Bryan, 2022), this research accentuates a useful perspective for organisations to protect their cyber realms and elongate their organisational lifespans.

The next section outlines the limitations of this research.

5.7 Research Limitations

This thesis, as with all other presentations of research, has certain limitations. The first limitation is owing to the enquiry logic to the research, which lends itself to limited generalisability. Similarly, the interpretative nature of the study may lead to certain ambiguities, which poses another limitation. Finally, as an emerging topic of research, it is still undergoing development and is limited by the other methodological choices for the study.

As with most research with an inductive logic, this research, too, may be limited in the generalisability of its findings and thus refers to external validity (Price and Murnan, 2004). This research was conducted with individuals who served as strategic decision-makers in both private and public sector organisations. These individuals represented organisations of varying dimensions as well as different industry sectors. This was an intentional choice to ensure the data collected was representative of the entire industry. However, another perspective to this choice translates into replicability of the results that may or may not be applicable to each of the industry sectors represented in the study, which is highlighted as an accepted limitation of qualitative studies (Wiersma, 2000). Thus, while care has been taken to present a panoramic view of the state of the industry, in certain organisations there may be the need to explore further.

Another limitation centres around the interpretative nature of the research, which is highly dependent on the chosen elite interview participants' understanding of the theme in question, coupled with the researcher's interpretation of the interviewees' responses. For instance, the understanding of competitive advantage through robust cybersecurity, discussed in the findings, relates to the interviewees' perceived appreciation of the concept rather than an informed quantitative figure derived from a performance statistic. While the practitioners' accounts are internally valid, through a future or different quantitative study, the findings may be understood to be somewhat dissimilar. This research is intended to widen the horizon for conversations of a similar nature, which enable a more comprehensive understanding of the specifics involved and lessen the gap of knowledge in this fast-evolving sphere of cybersecurity research.

The final limitation also owes itself to the methodological choices made during this study, which was conducted during the time the Covid-19 pandemic was underway, and the research was witness to the swift changes brought on by the pandemic and its significant impact on the field as such. Thus, through a cross-section in time, this study was able to obtain an all-around perspective of the various forces at play in the industry and the potential direction of its movement in the near future. A study of this nature thus does not include temporal comparisons (Jansen and Shipp, 2019), which may provide a potential future research avenue in this field. A longitudinal study, investigating the evolving world of organisational cybersecurity practices during and after the pandemic, would offer such findings. Similarly, while this study explores both the public sector and private sector organisations, most of the individuals interviewed belonged to the private sector. While the impact of inadequate cybersecurity as well as influence of strategic decision-makers in the discussion would be comparable, the specific impact may axiomatically differ.

Thus, despite the meticulousness of the researcher, the remedies of the findings may not have eliminated all researcher-related bias. However, the hallmarks of trustworthiness and credibility, as stated by Schwandt, Lincoln, and Guba (2007), have been ensured to follow methodological integrity, which would enable the findings to have justifiable and far-reaching impact in both academic and practitioner communities. Having briefly referred to these limitations, the next section details avenues for potential future research.

5.8 Further Research

At a moment in time of great historical significance posed by the 4.0 economy, coupled with the aftermath of the Covid-19 pandemic, the field of cybersecurity has witnessed unprecedented shifts. This thesis has intended to seize the opportunity that the confluence of this particular time period has provided, with the hope of exploring crucial answers to securing the organisational cyber realms. This fruitful exercise has thus revealed several instances for future research to expand the horizons of the field.

Since the field of cybersecurity relies heavily on modern technologies, which are in a constant state of evolution, the first opportunity for future research is necessitated by the very nature of technology. As the impact of digitalisation is yet revealing itself across different geographies and industry sectors, it may not yet be considered universally standardised. This further impacts organisational choice of strategies employed to secure its cyber realms. As technologies advance in their universal acceptance and influence, there is expected to be a parallel impact on cyber-assets and their vulnerabilities being exposed to a global audience. This would require research to keep pace with this evolving field instead of following the footsteps of technological advancement. As long as technologies advance faster than research explores them, the cyber-world - and thereby the world at large - would be a vulnerable domain. Discussing cyber-resilience (World Economic Forum and Accenture, 2023) and corporate digital responsibility (Lobschat *et al.*, 2021) are necessary, and academic research needs to explore modern phenomena such as ChatGPT (Van Dis *et al.*, 2023) and their impact on domains such as cybersecurity.

Another opportunity arises from the chosen sample of this study, which sought to cover a cross-section of the wide industry sectors to appreciate a realistic picture of the cybersecurity of organisations. This study underscores the intersections of common behavioural traits of organisations with respect to their craft and the implementation of their cyber strategy, and the afflictions of cyber vulnerabilities. Furthermore, in contemporary times, cyber realms are the spaces where most organisations keep their valuables for safekeeping - including all stakeholder information, organisational future plans, and other intellectual properties. This study confirms the exaggerated concerns of banking and financial, technological, and other critical infrastructure organisations, relative to others such as retail and hospitality. However, each of the sectors requires respective research to recognise the specific conditions and circumstances which make their cyber realm attractive to a cybercriminal, and ways to overcome the associated threats.

With respect to industry sectors, this study primarily explored the functioning of private sector organisations, including a few public sector firms as well. However, the concerns faced by the public sector - such as inadequate resources/funding, lack of leadership priority for cybersecurity and exposed vulnerabilities - making them a popular target of cybercriminals - warrants specific research conducted for this distinctive sector. Public sector enterprises may have even additional obstacles to overcome on the path to robust cybersecurity; yet the multitude of their stakeholders may be viewed as potential victims of future cyber-crimes, which merits adequate qualitative and quantitative research in the field, from which the stakeholders can benefit.

This research also highlighted the significant role played by regulations in the field of cybersecurity, especially made complicated on account of the lack of borders and jurisdictional concerns in the cyber realm. Is cybersecurity the responsibility of the organisation or the regulatory authority or the nation where the organisation is headquartered, or meant to be a public-private partnership or a universally followed policy across the globe? These questions also merit further research to be focussed on the unique association between regulations and strengthened cybersecurity. Answering some of these questions may serve as a starting point to exploring this helpful arena. This study has helped establish the importance of regulations in compelling some otherwise reluctant organisations to prioritise cybersecurity. This aspect may be another avenue to investigate this relationship, perhaps through a quantitative study which may help with the generalisability of findings.

Finally, this study underlines the dynamic nature of this ever-evolving field. This nature also restricts the education and further employment aspects of the field. The study highlighted the lack of adequate experience of board directors and other senior professionals in the field, owing to the relatively new genesis of the domain itself. This translates to the lack of adequate education and qualifications prevalent in the field, which further influences the skills-gap of personnel with necessary expertise in the field. This aspect of cybersecurity training and skills-gap impacting organisational futures may be assessed through future research examining the factual situation, the association between the two, and the impact of one over the other - with potential studies using an abductive logic.

5.9 Personal Reflection

Prior to embarking on this PhD journey, I had imagined that resuming an academic life after a decade-and-a-half in the corporate sector would involve learning certain skills and acquiring a degree. Yet, this doctoral journey has remarkably been more than the sum of its mere parts. As an inherently reflective and introspective individual, the evolving PhD journey has meant several iterations of this exercise. One of these reflections is associated with the impact of time and learning on the presumed plan for the thesis development, in the form of changing theoretical foundations of my research. Another is with respect to the challenges faced with my methodological choices, which have allowed me a deeper understanding of my strengths and a new perspective on the very nature of challenges. Finally, the third reflection relates to the significance of my immediate past on the long-term plans for my future, in terms of my PhD journey’s learning providing me clarity to the domain of my professional existence henceforth.

One of the significant realisations that I have reached at this juncture of the thesis is that learning of any nature - whether specific to doctoral studies or generic to research per se - is impossible to predict. Like the flow of a river which finds its own course, and also changes over a longer term, authentic learning is similarly possible only with an inherent liberty of practice. Since the stage of writing my PhD proposal till now, even the topic of my thesis has gone through a process of evolution. Similarly, while penning my review of literature, the primary theoretical influence was Stewardship Theory (Davis, Schoorman and Donaldson, 1997). The process of data collection, analysis, and discussion consequently (surprisingly for me) shifted the focal theoretical foundation away from this theory to the Resource-Based View (Wernerfelt, 1984). I have thus discovered that trustworthy research involves allowing the learning to be able to chart new courses, as yet not imagined or planned. For the purpose of the development of the field as well as that of the researcher, this is wonderful news.

The second reflection came upon me during the process of my data collection, which was rendered more challenging than presumed, on account of the global Covid-19 pandemic. An unprecedented phenomenon (for the past 100 years) such as this meant swift adaptation of the methodology and data collection techniques, while retaining the inherent philosophical standpoint and research logic. This translated to an even more challenging process of identifying, accessing, and engaging with corporate elites for my research than would have been in the ordinary course of events. While these sometimes felt insurmountable at first, I was pleasantly surprised to discover some inner strengths, which enabled me to explore alternative ways (which are detailed in Chapter 3) to maintain the high standards of my research yet fulfilling its objectives in novel ways. Thus, persistence to continue my attempts despite challenges, and the resilience to adapt consequently to the said challenges, are both significant strengths which I have unearthed during this unique quest. Furthermore, similar to Proposition 3 of my research findings, I have realised that the ability to adapt to challenges unearths undiscovered opportunities for personal and professional development.

The final reflection is the impact of the years of my PhD on perhaps the rest of my professional life and existence. Despite a successful career in the corporate sector, I was unable to find contentment in my profession, and through the trials and tribulations of my doctoral journey, I feel fortunate to have found my vocation. Inadvertently instrumental in this realisation are my mentors and supervisors who, through their stellar guidance, have set stratospheric standards for me as academics. It is thus abundantly clear to me to follow on that path, pursuing a career in academia devoted to continuing to expand my horizons through research, while simultaneously facilitating the metamorphosis of the younger learners of today into impactful leaders of tomorrow through teaching. I appreciate now that learning, similar to cybersecurity strategy, is an ongoing and ever-evolving process. The only way to offer a meaningful contribution to the field of knowledge and my students is to continue to learn, and that is a precious lesson for my journey henceforth. In other words, I have discovered the significance of strategic choices on the path to realising even an individual's unique advantage.

5.10 Chapter Summary

This chapter concludes this thesis, with the hope of shining a light on this fascinating arena where cybersecurity meets strategic decision-making. For a field as dynamic and constantly evolving, it is hoped that this thesis provides a stable foundation over which the edifice of future research - that helps both the academic and practitioner communities - may be erected. Having revealed some enigmas from the black box of the boardrooms to assist organisations find contemporary advantages over their competitors and widen the horizons of academic research in cybersecurity, the author shall continue on the quest for knowledge and exploration.

References

Aberbach, J.D. and Rockman, B.A. (2002) 'Conducting and coding elite interviews', *PS - Political Science and Politics*, 35(4), pp. 673–676. Available at: https://doi.org/10.1017/S1049096502001142.

Ablon, L. and Libicki, M. (2015). Hackers' Bazaar: The Markets for Cybercrime Tools and Stolen Data. Defense Counsel Journal, 82(2).

Abraham, C. and Sims, R.R. (2021) 'A Comprehensive Approach to Cyber Resilience', *MIT Sloan Management Review*, 62(4), pp. 1–4.

Accenture and Ponemon Institute LLC. (2010). How Global Organizations Approach the Challenge of Protecting Personal Data.

Accenture, 2010. Accenture | Let There Be Change. [online] Available at: https://microsite.accenture.com/dataprivacyreport/Documents/Accenture_Data_Privacy_Report.pdf [Accessed 31 May 2020].

Adams, R.B., Hermalin, B.E. and Weisbach, M.S. (2010) 'The role of boards of directors in corporate governance: A conceptual framework and survey', *Journal of Economic Literature*, 48(1), pp. 58–107. Available at: https://doi.org/10.1257/jel.48.1.58.

Adler, P.A. and Adler, P., 1994. Observational techniques.

Adner, R., Zemsky, P. (2006) 'A demand-based perspective on sustainable competitive advantage', *Strategic Management Journal*, 27(3), pp. 215–239. Available at: https://doi.org/10.1002/smj.513.

Alberts, D.S. and Papp, D.S., 1997. *The information age: An anthology on its impact and consequences*. Office of the Assistant Secretary of Defense Washington DC Command and Control Research Program (CCRP).

Alberts, D.S., 1996. *Defensive information warfare*. NATIONAL DEFENSE UNIV WASHINGTON DC INST FOR NATIONAL STRATEGIC STUDIES.

Aldasoro, I. *et al.* (2022) 'The drivers of cyber risk', *Journal of Financial Stability*, 60. Available at: https://doi.org/10.1016/j.jfs.2022.100989.

Allen, J. H., Crabb, G., Curtis, P. D., Fitzpatrick, B., Mehravari, N., and Tobar, D. (2015). Structuring the Chief Information Security Officer Organization. http://www.sei.cmu.edu

Alotaibi, F.M. and Vassilakis, V.G., 2021. Sdn-based detection of self-propagating ransomware: the case of BadRabbit. *IEEE Access*, *9*, pp.28039-28058.

Anderson, P. (1999) 'Complexity Theory and Organisation Science', *Organization Science*, 10(3), pp. 216–232. Available at: https://doi.org/10.1097/EDE.0b013e3181.

Andrew, J. and Baker, M., 2021. The general data protection regulation in the age of surveillance capitalism. *Journal of Business Ethics*, *168*, pp.565-578.

Andrews, K.R., 1981. Corporate strategy as a vital function of the board. *Harvard Business Review*, *59*(6), p.174.

Ansoff, H.I., 1987. The emerging paradigm of strategic behavior. *Strategic management journal*, *8*(6), pp.501-515.

Archibald, M.M. *et al.* (2019) 'Using Zoom Videoconferencing for Qualitative Data Collection: Perceptions and Experiences of Researchers and Participants', *International Journal of Qualitative Methods*, 18. Available at: https://doi.org/10.1177/1609406919874596.

Arend, R.J. and Lévesque, M. (2010) 'Is the resource-based view a practical organizational theory?', *Organization Science*, 21(4), pp. 913–930. Available at: https://doi.org/10.1287/orsc.1090.0484.

Armstrong, R.C. and Mayo, J.R. (2009) 'Leveraging complexity in software for cybersecurity', *ACM International Conference Proceeding Series* [Preprint]. Available at: https://doi.org/10.1145/1558607.1558643.

Arquilla, J. and Ronfeldt, D. (1997) 'CyberWar is Coming', in *In Athena's Camp: Preparing for Conflict in the Information Age*.

Ashraf, M. (2022) 'The Role of Peer Events in Corporate Governance: Evidence from Data Breaches', *Accounting Review*, 97(1), pp. 1–24. Available at: https://doi.org/10.2308/TAR-2019-1033.

Axelrod, C. W. (2015). Cybersecurity and modern tactical systems. Crosstalk, 4–11. https://www.researchgate.net/publication/298822817

Bain, J.S. (1959) *Industrial Organization: A Treatise.* 2nd Edition, John Wiley, London.

Balitzer, S. (2016) 'What Common Law and Common Sense Teach us about Corporate Cybersecurity', *University of Michigan, Journal of Law Reform,* 49:4.

Bana, S. H., Brynjolfsson, E., Jin, W., Steffen, S., and Wang, X. (2022). Human Capital Acquisition in Response to Data Breaches. Workshop on the Economics of Information Security. https://www.weforum.org/agenda/2019/04/how-much-data-is-generated-each-day-cf4bddf29f/,

Banalieva, E. R. and Dhanaraj, C. (2019). Internalization theory for the digital economy. Journal of International Business Studies, 50(8), 1372–1387. https://doi.org/10.1057/s41267-019-00243-7

Barnard-Wills, D. and Ashenden, D., 2012. Securing virtual space: Cyber war, cyber terror, and risk. *Space and Culture*, *15*(2), pp.110-123.

Barnes, C. (2019) 'Protecting Lives, Data and ROI by Integrating Physical and Cybersecurity', *Connected Copy*.

Barney, J. (1991) 'Firm Resources and Sustained Competitive Advantage', *Journal of Management,* 17(1), pp. 99–120. Available at: https://doi.org/10.1177/014920639101700108.

Barney, J. B. (1995). Looking inside for competitive advantage. Academy of Management Perspectives, 9(4), 49–61. https://doi.org/10.5465/ame.1995.9512032192

Barney, J., Wright, M. and Ketchen, D.J. (2001) 'The resource-based view of the firm: Ten years after 1991', *Journal of Management,* 27, pp. 625–641.

Barney, J.B. (2001) 'Resource-based theories of competitive advantage: A ten-year retrospective on the resource-based view', *Journal of Management,* 27(6), pp. 643–650. Available at: https://doi.org/10.1016/S0149-2063(01)00115-5.

Barney, J.B., and Clark, D.N. (2007) 'Resource-Based Theory', in *Resource Based Theory: Creating and Sustaining Competitive Advantage*, pp. 3–75.

Barney, J.B., and Clark, D.N. (2007a) 'Information Technology as a Source of Sustained Competitive Advantage', in *Resource Based Theory: Creating and Sustaining Competitive Advantage*.

Barney, J.B., and Clark, D.N. (2007b) ‘Resource-Based Theory’, in *Resource Based Theory: Creating and Sustaining Competitive Advantage,* pp. 3–75.

Barney, J.B., and Clark, D.N. (2007c) ‘The future of resource-based theory’, in *Resource Based Theory: Creating and Sustaining Competitive Advantage,* pp. 247–263.

Barney, J.B. and Zajac, E.J. (1994) ‘Competitive Organizational Behavior: Toward an Organizationally-based Theory of Competitive Advantage’, *Strategic Management Journal,* 15, pp. 5–9.

Barroso-castro, C., Villegas-peri, M.M. and Dominguez, M. (2017) ‘Board members’ contribution to strategy : The mediating role of board internal processes’, *European Research on Management and Business Economics,* 23, pp. 82–89. Available at: https://doi.org/10.1016/j.iedeen.2017.01.002.

Batra, A. (2020) ‘Cyber Security Management: Creating Governance, Risk, and Compliance Framework’, *i-manager’s Journal on Software Engineering,* 14(4), p. 27. Available at: https://doi.org/10.26634/jse.14.4.17403.

Beck, U., 1992. From industrial society to the risk society: Questions of survival, social structure, and ecological enlightenment. *Theory, culture & society*, *9*(1), pp.97-123.

Becker, G.S. (1964) Human Capital: A Theoretical and Empirical Analysis with Special Reference to Education. 3rd Edition, *The University of Chicago Press*, Chicago.

Bejan, F. (2022) ‘Cybersecurity and Cybercrime: Challenges of an Invisible Space’, *Perspective of Law and Public Administration,* 11(1).

Bennett, D., Barrett, A. and Helmich, E. (2019) ‘How to…analyse qualitative data in different ways’, *Clinical Teacher,* 16(1), pp. 7–12. Available at: https://doi.org/10.1111/tct.12973.

Berle, A.A., 1932. A., MEANS, G., C., 1933: The Modern Corporation and Private Property. *University of Pennsylvania Law Review and American Law Register*, *81*(6), pp.782-785.

Bernard, H.R., Pelto, P.J., Werner, O., Boster, J., Romney, A.K., Johnson, A., Ember, C.R. and Kasakoff, A., 1986. The construction of primary data in cultural anthropology. *Current Anthropology*, *27*(4), pp.382-396.

Biddle, B.J., 1986. Recent developments in role theory. *Annual review of sociology*, *12*(1), pp.67-92.

Biedenbach, T. and Jacobsson, M. (2016) 'The Open Secret of Values: The Roles of Values and Axiology in Project Research', *Project Management Journal*, 47(3), pp. 139–155. Available at: https://doi.org/10.1177/875697281604700312.

Blaikie, N., 2007. Approaches to social enquiry: Advancing knowledge. Polity.

Blaikie, N. (2018) 'Confounding issues related to determining sample size in qualitative research', *International Journal of Social Research Methodology*, 21(5), pp. 635–641. Available at: https://doi.org/10.1080/13645579.2018.1454644.

Bleier, A., Goldfarb, A. and Tucker, C., 2020. Consumer privacy and the future of data-based innovation and marketing. *International Journal of Research in Marketing*, *37*(3), pp.466-480.

Boeker, W., 1989. Strategic change: The effects of founding and history. *Academy of Management journal*, *32*(3), pp.489-515.

Bonnafous-Boucher, M. and Porcher, S. (2010) 'Towards a Stakeholder Society: Stakeholder theory vs Theory of Civil Society', *European Management Review*, 7, pp. 205–216.

Bower, J.L., 1972. *Managing the resource allocation process: A study of corporate planning and investment*. Homewood: Irwin.

Bowling, B. and Ross, J., 2006. SOCA: The Serious and Organised Crime Agency.

Bowman, C. and Ambrosini, V. (2003) 'How the Resource-based and the Dynamic Capability Views of the Firm Inform Corporate-level Strategy', *British Journal of Management*, 14(4), pp. 289–303. Available at: https://doi.org/10.1111/j.1467-8551.2003.00380.x.

Bowman, E.H. and Hurry, D. (1993) 'Strategy through the Option Lens: An Integrated View of Resource Investments and the Incremental-Choice Process', *The Academy of Management Review*, 18(4), pp. 760–782.

Boyes, H. (2015). Cybersecurity and Cyber-Resilient Supply Chains. Technology Innovation Management Review, 28–34. www.timreview.ca

Boyes, H. (2015a) 'Cybersecurity and Cyber-Resilient Supply Chains', *Technology Innovation Management Review*, pp. 28–34. Available at: www.timreview.ca.

Boyes, H. (2015b) ‘Cybersecurity and Cyber-Resilient Supply Chains’, *Technology Innovation Management Review* [Preprint]. Available at: www.timreview.ca.

Brantly, A. F. (2014). Cyber Actions by State Actors: Motivation and Utility. International Journal of Intelligence and Counterintelligence, 27(3), 465–484. https://doi.org/10.1080/08850607.2014.900291

Braun, V. and Clarke, V. (2008) ‘Using thematic analysis in psychology’, *Qualitative Research in Psychology*, 3(2), pp. 77–101. Available at: http://www.tandfonline.com/action/journalInformation?journalCode=uqrp20%5Cnhttp://www.tandfonline.com/action/journalInformation?journalCode=uqrp20.

Brenner, S.N., 1993, July. The stakeholder theory of the firm and organizational decision making: Some propositions and a model. In Proceedings of the International Association for Business and Society (Vol. 4, pp. 405-416).

Broeders, D. (2016) The public core of the Internet: An International Agenda for Internet Governance.

Bronk, C. and Tikk-Ringas, E., 2013. The cyber-attack on Saudi Aramco. *Survival*, *55*(2), pp.81-96.

Browdie, B. (2013). Best Incentive to Shore Up Cybersecurity? Trust, Bank Group Says. In From: American Banker (Vol. 178). http://www.sourcemedia.com/

Bryman, A., 2008. The end of the paradigm wars. *The SAGE handbook of social research methods*, pp.13-25.

Brynjolfsson, E. and McAfee, A., 2012. *Race against the machine: How the digital revolution is accelerating innovation, driving productivity, and irreversibly transforming employment and the economy*.

Burgelman, R.A., 1983. A model of the interaction of strategic behavior, corporate context, and the concept of strategy. *Academy of management Review*, *8*(1), pp.61-70.

Cabinet Office, 2009. *Cybersecurity strategy of the United Kingdom: safety, security, and resilience in cyber space.* Retrieved from www. Cabinetoffice.gov.uk/media/216620/css0906.pdf

Cadbury, A., 1992. *Report of the committee on the financial aspects of corporate governance* (Vol. 1). Gee.

Caers, R., Bois, C.D., Jegers, M., Gieter, S.D., Schepers, C. and Pepermans, R., 2006. Principal-agent relationships on the stewardship-agency axis. *Nonprofit Management and Leadership*, *17*(1), pp.25-47.

Carey, D.C. and Patsalos-fox, M. (2006) 'Shaping Strategy from the Boardroom', *The McKinsey Quarterly*, (3), pp. 110–115.

Carnahan, S., Agarwal, R. and Campbell, B. (2010) 'The Effect of Firm Compensation Structures on the Mobility and Entrepreneurship of Extreme Performers', *Business*, 30(12), pp. 1–43. Available at: https://doi.org/10.1002/smj.

Carpenter, M.A. (2016) 'The Strategic Context of External Network Ties: Examining the Impact of Director Appointments on Board Involvement in Strategic Decision-Making Author (s): Mason A . Carpenter and James D. Westphal Published by : Academy of Management Stable URL : http,' *Academy of Management Journal*, 44(4), pp. 639–660.

Carr, M., 2015. Power plays in global internet governance. *Millennium*, *43*(2), pp.640-659.

Carson, R., 1962. Silent spring III. *New Yorker, 23*.

Carver, J., 2000. Remaking Governance. *American School Board Journal*, *187*(3), pp.26-30.

Cassell, C. *et al.* (2005) *Qualitative Management Research: A Thematic Analysis of Interviews with Stakeholders in the Field, ESRC Benchmarking good practice in qualitative management research*. Available at: https://doi.org/10.1109/PESC.2004.1355184.

Castells, M., 1989. Social movements and the informational city. *Hitotsubashi journal of social studies*, *21*(1), pp.197-206.

Catteddu, D. and Hogben, G., 2009. ABOUT ENISA. *Cloud Computing: Benefits, risks, and recommendations for information security*.

Cerin, B. (2020) 'Cyber security risk is a board-level issue', in *2020 43rd International Convention on Information, Communication and Electronic Technology, MIPRO 2020 - Proceedings*. Institute of Electrical and Electronics Engineers Inc., pp. 384–388. Available at: https://doi.org/10.23919/MIPRO48935.2020.9245151.

Chandler, A.D., 1962. Strategy and structure: Chapters in the history of the industrial empire. *Cambridge Mass*.

Chartered Governance Institute (2022) *FTSE 350 Boardroom Bellwether*.

CHASE, S., 2005. E (2005): Narrative inquiry: Multiple lenses, approaches, voices. *The Sage Handbook of Qualitative Research. London: SAGE Publications*.

Cheffins, B.R. (2001) 'History and the global corporate governance revolution: The UK perspective', *Business History*, 43(4), pp. 87–118. Available at: https://doi.org/10.1080/713999243.

Cheffins, B.R. (2015) 'Corporate Governance since the Managerial Capitalism Era', *Business History Review*, 89(4), pp. 717–744. Available at: https://doi.org/10.1017/S0007680515000690.

Cheffins, B.R., 1999. Teaching corporate governance. *Legal studies*, *19*(4), pp.515-525.

Chertoff, M. (2008) 'The cybersecurity challenge', *Regulation and Governance*, 2(4), pp. 480–484. Available at: https://doi.org/10.1111/j.1748-5991.2008.00051.x.

Chiasson, P. (2005) 'Abduction as an Aspect of Retroduction', *The Commens Encyclopedia* [Preprint].

Chng, S., Lu, H. Y., Kumar, A., and Yau, D. (2022). Hacker types, motivations, and strategies: A comprehensive framework. In Computers in Human Behavior Reports (Vol. 5). Elsevier Ltd. https://doi.org/10.1016/j.chbr.2022.100167

Cisco and affiliates (2023) *Cisco 2023 Data Privacy Benchmark Study*. Available at: https://www.cisco.

Clarkson, M.E., 1995. A stakeholder framework for analyzing and evaluating corporate social performance. Academy of management review, 20(1), pp.92-117.

Clarysse, B., Knockaert, M. and Lockett, A. (2007) 'Outside board members in high tech start-ups', *Small Business Economics*, 29(3), pp. 243–259. Available at: https://doi.org/10.1007/s11187-006-9033-y.

Clendenin, W.D. (1972) 'Company Presidents Look at Board Directors', *California Management Review*, 14(3), pp. 60–66.

Coff, R. and Kryscynski, D., 2011. Invited editorial: Drilling for micro-foundations of human capital–based competitive advantages. *Journal of management*, *37*(5), pp.1429-1443.

Coff, R.W., 1997. Human assets and management dilemmas: Coping with hazards on the road to resource-based theory. *Academy of management review*, *22*(2), pp.374-402.

Conteh, N. Y., and Schmick, P. J. (2016). Cybersecurity:risks, vulnerabilities, and countermeasures to prevent social engineering attacks. International Journal of Advanced Computer Research, 6(23), 31–38. https://doi.org/10.19101/ijacr.2016.623006

Corallo, A., Lazoi, M. and Lezzi, M. (2020) 'Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts', *Computers in Industry*, 114, p. 103165. Available at: https://doi.org/10.1016/j.compind.2019.103165.

Corbin, J.M. and Strauss, A., 1990. Grounded theory research: Procedures, canons, and evaluative criteria. *Qualitative sociology*, *13*(1), pp.3-21.

Cordes, F. and Stacey, N. (2017) 'Is UK Industry ready for the Fourth Industrial Revolution?', *BCG: The Boston Consulting Group: Boston, MA, USA* [Preprint]. Available at: https://doi.org/10.1209/0295-5075/3/1/012.

Corley, K.G. and Gioia, D.A. (2011) 'Building Theory about Theory Building: What Constitutes a Theoretical Contribution?', *The Academy of Management Review*, 36(1), pp. 12–32. Available at: https://about.jstor.org/terms.

Corradini, I., and Nardelli, E. (2020). Advances in Human Factors in Cybersecurity. In I. Corradini, E. Nardelli, and T. Ahram (Eds.), AHFE 2020 Virtual Conference on Human Factors in Cybersecurity. http://www.springer.com/series/11156

Council, F.R. (2018) *THE UK CORPORATE GOVERNANCE CODE*.

Courtney, H., Kirkland, J. and Viguerie, P., 1997. Strategy under uncertainty. *Harvard business review*, *75*(6), pp.67-79.

Craig, A.N., Shackelford, S.J. and Hiller, J.S. (2015) 'Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis', *American Business Law Journal*, 52(4), pp. 721–787. Available at: https://doi.org/10.1111/ablj.12055.

Craigen, D., Diakun-Thibault, N. and Purse, R. (2014) ‘Defining Cybersecurity’, *Technology Innovation Management Review* [Preprint]. Available at: www.timreview.ca.

Creswell, J.W. and Miller, D.L. (2000) ‘Determining Validity in Qualitative Inquiry’, *Theory Into Practice*, 39(3), pp. 124–130.

Creswell, J.W. *et al.* (2007) ‘Qualitative Research Designs: Selection and Implementation’, *The Counseling Psychologist*, 35(2), pp. 236–264. Available at: https://doi.org/10.1177/0011000006287390.

Cristea, L. M. (2020). Current security threats in the national and international context. JOURNAL OF ACCOUNTING AND MANAGEMENT INFORMATION SYSTEMS, 19(2), 351–378. https://doi.org/10.24818/jamis.2020.02007

Crotty, M.J., 1998. The foundations of social research: Meaning and perspective in the research process. *The foundations of social research*, pp.1-256.

Cuomo, F., Mallin, C. and Zattoni, A. (2016) ‘Corporate Governance Codes: A Review and Research Agenda’, *Corporate Governance: An International Review*, 24(3), pp. 222–241. Available at: https://doi.org/10.1111/corg.12148.

Czarniawska, B., 2004. *Narratives in social science research*. Sage.

Daily, M., Dalton, D.R. and Jr., A.A.C. (2003) ‘Corporate Governance : Decades of Dialogue and Data’, *Academy of Management Review*, 28(3), pp. 371–382.

D'Amato, D., Droste, N., Allen, B., Kettunen, M., Lähtinen, K., Korhonen, J., Leskinen, P., Matthies, B.D. and Toppinen, A., 2017. Green, circular, bio economy: A comparative analysis of sustainability avenues. *Journal of cleaner production*, *168*, pp.716-734.

Danyk, Y., Maliarchuk, T. and Briggs, C. (2017) ‘Hybrid War: High-tech, Information and Cyber Conflicts’, *Connections: The Quarterly Journal*, 16(2), pp. 5–24. Available at: https://doi.org/10.11610/connections.16.2.01.

Darwin, C. and Darwin, C.R., 1909. *The origin of species* (pp. 95-96). New York: PF Collier & son.

Davies, D. and Dodd, J. (2002) ‘Pearls, Pith, and Provocation Qualitative Research and the Question of Rigor’, *Qualitative Health Research*, 12(2), pp. 279–289.

Davis, J.H., Schoorman, F.D. and Donaldson, L., 1997. Toward a stewardship theory of management. *Academy of Management review*, *22*(1), pp.20-47.

Davis, K., 1973. The case for and against business assumption of social responsibilities. *Academy of Management journal*, *16*(2), pp.312-322.

De Minville, M. (2020) ‘Corporate Governance and Digital Responsibility’, in *Cybersecurity and Decision Makers*. Available at: http://ebookcentral.proquest.com/lib/reading/detail.action?docID=6173684.

Del, G. *et al.* (2013) ‘The Rise of Corporate Governance in the UK: When and Why’, *Current Legal Problems*, (270), p. 2305.

Demb, A. and Neubauer, F.-F. (1992) ‘The Corporate Board: Confronting the Paradoxes’, *Long Range Planning*, 25(3), pp. 9–20.

Der Derian, J., 2000. Virtuous war/virtual theory. *International affairs*, *76*(4), pp.771-788.

Devers, K. (1999) ‘How will we know “good” qualitative research when we see it? Beginning the dialogue in health services research,’ *Health Services Research* , pp. 1153–1188.

Devers, K.J. and Frankel, R.M. (2000) ‘Study design in Qualitative research - 2: Sampling and data collection strategies’, *Education for Health*, 13(2), pp. 263–271. Available at: https://doi.org/10.1080/13576280050074543.

Dicce, R.P. and Ewers, M.C. (2020) ‘Becoming Linked In: Leveraging Professional Networks for Elite Surveys and Interviews’, *Geographical Review*, 110(1–2), pp. 160–171. Available at: https://doi.org/10.1111/gere.12346.

DiMaggio, P.J. and Powell, W.W., 1983. The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American sociological review*, pp.147-160.

Dobák, I. (2021) ‘Thoughts on the evolution of national security in cyberspace’, *Security and Defence Quarterly*, 33(1), pp. 75–85. Available at: https://doi.org/10.35467/sdq/133154.

Donaldson, L., and Davis, J.H., 1991. Stewardship theory or agency theory: CEO governance and shareholder returns. *Australian Journal of management*, *16*(1), pp.49-64.

Donaldson, L., 1990. The ethereal hand: Organizational economics and management theory. *Academy of management Review*, *15*(3), pp.369-381.

Dosi, G., 1988. Sources, procedures, and microeconomic effects of innovation. *Journal of economic literature*, pp.1120-1171.

Drazin, R. and Van de Ven, A.H., 1985. Alternative forms of fit in contingency theory. *Administrative science quarterly*, pp.514-539.

Drisko, J.W. (1997) 'Strengthening qualitative studies and reports: Standards to promote academic integrity', *Journal of Social Work Education*, 33(1), pp. 185–197. Available at: https://doi.org/10.1080/10437797.1997.10778862.

Dulewicz, V. and Herbert, P., 2004. Does the composition and practice of boards of directors bear any relationship to the performance of their companies?. *Corporate Governance: An International Review*, *12*(3), pp.263-280.

Dumay, J., 2016. A critical reflection on the future of intellectual capital: from reporting to disclosure. *Journal of Intellectual capital*, *17*(1), pp.168-184.

Eby, L.T., Hurst, C.S. and Butts, M.M., 2009. The redheaded stepchild in organizational and social science research. *Statistical and methodological myths and urban legends: Doctrine, verity and fable in the organizational and social sciences*, pp.219-246.

Eisenhardt, K.M. (1989) 'Building Theories from Case Study Research', *The Academy of Management Review*, 14(4), pp. 532–550.

Eisenhardt, K.M. and Brown, S.L., 1998. Competing on the edge: Strategy as structured chaos. *Long range planning*, *31*(5), pp.786-789.

Eisenhardt, K.M. and Martin, J.A. (2000) 'Dynamic capabilities: What are they?', *Strategic Management Journal*, 21(10–11), pp. 1105–1121. Available at: https://doi.org/10.1002/1097-0266(200010/11)21:10/11<1105::AID-SMJ133>3.0.CO;2-E.

Eisenhardt, K.M., 1988. Agency-and institutional-theory explanations: The case of retail sales compensation. *Academy of Management journal*, *31*(3), pp.488-511.

Elahi, E. (2013) 'Risk management: The next source of competitive advantage', *Foresight*, 15(2), pp. 117–131. Available at: https://doi.org/10.1108/14636681311321121.

Ellstrand, A.E., Tihanyi, L. and Johnson, J.L., 2002. Board structure and international political risk. *Academy of Management Journal*, *45*(4), pp.769-777.

Enjolras, M., Camargo, M. and Schmitt, C. (2019) ‘Are High-Tech Companies More Competitive Than Others? An Empirical Study of Innovative and Exporting French SMEs,’ *Technology Innovation Management Review*, 9(1), pp. 33–48. Available at: https://doi.org/10.22215/timreview/1210.

Eriksson, J. and Giacomello, G. (2006) ‘The information revolution, security, and international relations: (IR)relevant theory?’, *International Political Science Review*, 27(3), pp. 221–244. Available at: https://doi.org/10.1177/0192512106064462.

Eriksson, J., 2001. Cyberplagues, IT, and security: Threat politics in the information age. *Journal of Contingencies and Crisis Management*, *9*(4), pp.200-210.

Eugen, P. (2018) ‘Exploring the New Era of Cybersecurity Governance’, *Ovidius University Annals: Economic Sciences Series*, XVIII(1), pp. 358–363.

Everard, J., 2000. *Virtual states*. Routledge.

Faludi, A. (1989) ‘Conformance vs. Performance: Implications for evaluation’, *Impact Assessment*, 7(2–3), pp. 135–151. Available at: https://doi.org/10.1080/07349165.1989.9726017.

Fama, E.F. and Jensen, M.C., 1983. Agency problems and residual claims. *The journal of law and Economics*, *26*(2), pp.327-349.

Fama, E.F., 1980. Agency problems and the theory of the firm. *Journal of political economy*, *88*(2), pp.288-307.

Farrar, J.H. (1999) ‘A Brief Thematic History of Corporate Governance’, *Bond Law Review*, 11(2), pp. 33–42. Available at: https://doi.org/10.4324/9780429354793-4.

Ferrillo, P.A. (2014) ‘Cybersecurity, Cyber Governance, and Cyber Insurance: What Every Director Needs to Know’, *Corporate Governance Advisor*, 22(5).

Filatotchev I. (2007). Corporate governance and the firm’s dynamics: Contingencies and complementarities. *Journal of Management Studies*, 44(6), 1041–1056.

Filatotchev, I., Toms, S. and Wright, M., 2006. The firm's strategic dynamics and corporate governance life-cycle. *International Journal of Managerial Finance*, *2*(4), pp.256-279.

Finkelstein, S. and D'aveni, R.A., 1994. CEO duality as a double-edged sword: How boards of directors balance entrenchment avoidance and unity of command. *Academy of Management journal*, *37*(5), pp.1079-1108.

Finnemore, M. and Hollis, D.B. (2016) 'Constructing Norms for Global Cybersecurity', *The American Journal of International Law*, 110(3), pp. 425–479.

Fiore, B., Ha, K., Huynh, L., Falcon, J., Vendiola, R. and Li, Y., 2023, March. Security Analysis of Ransomware: A Deep Dive into WannaCry and Locky. In *2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 285-294). IEEE.

Flick, U., Von Kardorff, E. and Steinke, I., 2004. What is qualitative research? An introduction to the field. *A companion to qualitative research*, *1*, pp.3-11.

Folta, T.B., 1998. Governance and uncertainty: the trade-off between administrative control and commitment. *Strategic management journal*, *19*(11), pp.1007-1028.

Forbes, D., and Milliken, F.J. (1999) 'Cognition and Corporate Governance : Understanding Boards of Directors as Strategic Decision-Making Groups', *The Academy of Management Review*, 24(3), pp. 489–505.

Formosa, P., Wilson, M., and Richards, D. (2021). A principalist framework for cybersecurity ethics. Computers and Security, 109. https://doi.org/10.1016/j.cose.2021.102382

Frankel, R. and Devers, K., 2000. Qualitative Research: a consumer′ s guide. *Education for health*, *13*(1), pp.113-123.

Frederick, W.C., 1994. From CSR1 to CSR2: The maturing of business-and-society thought. *Business & Society*, *33*(2), pp.150-164.

Freeman, R.E., 1984. *Strategic management: A stakeholder approach*. Cambridge university press.

Freeman, R.E., Harrison, J.S., Wicks, A.C., Parmar, B.L. and De Colle, S., 2010. Stakeholder theory: The state of the art.

Frooman, J. (1999) ‘Stakeholder Influence Strategies’, *The Academy of Management Review*, 24(2), pp. 191–205.

Fulford, H. and Doherty, N.F. (2003) ‘The application of information security policies in large UK-based organizations: An exploratory investigation’, *Information Management and Computer Security*, 11(2–3), pp. 106–114. Available at: https://doi.org/10.1108/09685220310480381.

Furnell, S.M. and Warren, M.J., 1999. Computer hacking and cyber terrorism: The real threats in the new millennium?. *Computers & Security*, *18*(1), pp.28-34.

Gale, M., Bongiovanni, I. and Slapnicar, S. (2022) ‘Governing cybersecurity from the boardroom: Challenges, drivers, and ways ahead’, *Computers and Security*, 121. Available at: https://doi.org/10.1016/j.cose.2022.102840.

Gandhi, G. (2014) ‘Complexity Theory in Cybersecurity’, (May), pp. 1–7.

Garg, S. and Eisenhardt, K.M. (2017) ‘Unpacking the CEO-Board relationship: How strategy making happens in entrepreneurial firms’, *Academy of Management Journal*, 60(5), pp. 1828–1858. Available at: https://doi.org/10.5465/amj.2014.0599.

Geers, K., Kindlund, D., Moran, N. and Rachwald, R., 2014. World War C: Understanding nation-state motives behind today’s advanced cyber-attacks. *FireEye, Milpitas, CA, USA, Tech. Rep., Sep*.

Gerber, M., von Solms, R. and Overbeek, P., 2001. Formalizing information security requirements. *Information Management & Computer Security*, *9*(1), pp.32-37.

Gerber, M., von Solms, R. and Overbeek, P., 2001. Formalizing information security requirements. *Information Management & Computer Security*, *9*(1), pp.32-37.

Ghemawat, P., 1991. *Commitment*. Simon and Schuster.

Ghezzi, A. (2013) *Revisiting business strategy under discontinuity, Management Decision*. Available at: https://doi.org/10.1108/MD-05-2012-0388.

Gibson, W., 2019. Neuromancer (1984). In *Crime and Media* (pp. 86-94). Routledge.

Gil, S., Kott, A. and Barabási, A.L. (2014) 'A genetic epidemiology approach to cyber-security', *Scientific Reports*, 4, pp. 1–8. Available at: https://doi.org/10.1038/srep05659.

Glinkowska, B. and Kaczmarek, B. (2015) 'Classical and Modern Concepts of Corporate Governance (Stewardship Theory and Agency Theory)', *Management*, 19(2), pp. 84–93. Available at: https://doi.org/10.1515/manment-2015-0015.

Godambe, V.P., 1982. Estimation in survey sampling: robustness and optimality. *Journal of the American Statistical Association*, *77*(378), pp.393-403.

Goergen, M. and Renneboog, L. (2014) 'Inside the board room', *Journal of Corporate Finance*, 28, pp. 1–5. Available at: https://doi.org/10.1016/j.jcorpfin.2014.05.004.

Golden, B.R. and Zajac, E.J. (2001) 'When will boards influence strategy? Inclination × power = strategic change,' *Strategic Management Journal*, 22(12), pp. 1087–1111. Available at: https://doi.org/10.1002/smj.202.

Goldstein, K. (2002) 'Getting in the door: Sampling and completing elite interviews', *PS - Political Science and Politics*, 35(4), pp. 669–672. Available at: https://doi.org/10.1017/S1049096502001130.

Goodpaster, K.E., 1991. Business ethics and stakeholder analysis. *Business ethics quarterly*, pp.53-73.

Goulding, C. (2005) 'Grounded theory, ethnography and phenomenology: A comparative analysis of three qualitative strategies for marketing research', *European Journal of Marketing*, 39(3-4 SPEC. ISS.), pp. 294–308. Available at: https://doi.org/10.1108/03090560510581782.

Granovetter, M., 1992. Economic institutions as social constructions: a framework for analysis. *Acta sociologica*, *35*(1), pp.3-11.

Grant, K. *et al.* (2014) 'Risky business: Perceptions of e-business risk by UK small and medium sized enterprises (SMEs)', *International Journal of Information Management*, 34(2), pp. 99–122. Available at: https://doi.org/10.1016/j.ijinfomgt.2013.11.001.

Grant, R.M., 1996. Prospering in dynamically-competitive environments: Organizational capability as knowledge integration. *Organization science*, *7*(4), pp.375-387.

Gray, L.M. *et al.* (2020) 'Expanding qualitative research interviewing strategies: Zoom video communications', *Qualitative Report*, 25(5), pp. 1292–1301.

Grove, H. and Clouse, M. (2017) 'Corporate governance for trillion-dollar opportunities', *Corporate Board: role, duties, and composition*, 13(3), pp. 19–27. Available at: https://doi.org/10.22495/cbv13i3art2.

Guetzkow, H., 1950. Long range research in international relations. *American Perspective*, *4*(4), pp.421-440.

Guillemin, M. and Gillam, L. (2004) 'Ethics, reflexivity, and "Ethically important moments" in research', *Qualitative Inquiry*, 10(2), pp. 261–280. Available at: https://doi.org/10.1177/1077800403262360.

Guthrie, J., Ricceri, F. and Dumay, J., 2012. Reflections and projections: a decade of intellectual capital accounting research. *The British accounting review*, *44*(2), pp.68-82.

Hagendorff, T., 2020. The ethics of AI ethics: An evaluation of guidelines. *Minds and machines*, *30*(1), pp.99-120.

Haleem, A. *et al.* (2022) 'Perspectives of cybersecurity for ameliorative Industry 4.0 era: a review-based framework', *Industrial Robot*, 49(3), pp. 582–597. Available at: https://doi.org/10.1108/IR-10-2021-0243.

Hall, R. (1993). A framework linking intangible resources and capabilities to sustainable competitive advantage. Strategic Management Journal, 14(8), 607–618. https://doi.org/10.1002/smj.4250140804

Hambrick, D.C. and Abrahamson, E., 1995. Assessing managerial discretion across industries: A multimethod approach. *Academy of Management Journal*, *38*(5), pp.1427-1441.

Hamel, G. and Prahalad, C.K., 1990. Strategic intent. *McKinsey quarterly*, (1), pp.36-61.

Hamilton, H.E., Tannen, D. and Schiffrin, D., 2015. *The handbook of discourse analysis*. John Wiley & Sons.

Hammersley, M., 2015. On ethical principles for social research. *International journal of social research methodology*, *18*(4), pp.433-449.

Harrison, J.S., Bosse, D.A. and Phillips, R.A., 2010. Managing for stakeholders, stakeholder utility functions, and competitive advantage. *Strategic management journal*, *31*(1), pp.58-74.

Hart, S.L. (1992) 'An Integrative Framework for Strategy-Making Processes', *Academy of Management Review*, 17(2), pp. 327–351.

Hartman, R.S., 1961. The logic of value. *The Review of Metaphysics*, pp.389-432.

Hartmann, C. C. and Carmenate, J. (2021). Academic research on the role of corporate governance and IT expertise in addressing cybersecurity breaches: Implications for practice, policy, and research. Current Issues in Auditing, 15(2), A9–A23. https://doi.org/10.2308/CIIA-2020-034

Harvey, W.S. (2011) 'Strategies for conducting elite interviews', *Qualitative Research*, 11(4), pp. 431–441. Available at: https://doi.org/10.1177/1468794111404329.

Hayes, R.H. (1985) 'Strategic planning: Forward in reverse?', *Harvard Business Review*, (Nov/Dec), pp. 111–119.

Heemskerk, E.M., Heemskerk, K. and Wats, M.M. (2017) 'Conflict in the boardroom: a participant observation study of supervisory board dynamics', *Journal of Management and Governance*, 21(1), pp. 233–263. Available at: https://doi.org/10.1007/s10997-015-9339-8.

Heimer, C. and Valeur, C., 2016. The digitally literate board–Science fiction, or just around the corner.

Hendry, K., and Kiel, G.C. (2004) 'The role of the board in firm strategy: Integrating agency and organisational control perspectives', *Corporate Governance: An International Review*, 12(4), pp. 500–520. Available at: https://doi.org/10.1111/j.1467-8683.2004.00390.x.

Hendry, K.P., Kiel, G.C. and Nicholson, G. (2010) 'How Boards Strategise: A Strategy as Practice View', *Long Range Planning*, 43(1), pp. 33–56. Available at: https://doi.org/10.1016/j.lrp.2009.09.005.

Henke Jr, J.W., 1986. Involving the board of directors in strategic planning. *Journal of Business Strategy*, *7*(2), pp.87-95.

Henry, R. and Peartree, C.E., 1998. Military theory and information warfare. *The US Army War College Quarterly: Parameters*, *28*(3), p.10.

Hermalin, B.E. (2005) ‘Trends in Corporate Governance’, *The Journal of Finance,* 60(5), pp. 2351–2384.

Herman, E.S., 1981. *Corporate control, corporate power* (Vol. 98, p. 1). New York: Cambridge University Press.

Hillman, A.J. and Dalziel, T., 2003. Boards of directors and firm performance: Integrating agency and resource dependence perspectives. *Academy of Management review, 28*(3), pp.383-396.

Hillman, A.J., Withers, M.C., and Collins, B.J. (2009) ‘Resource dependence theory: A review’, *Journal of Management*, 35(6), pp. 1404–1427. Available at: https://doi.org/10.1177/0149206309343469.

Hilmer, F.G., 1993. The governance research agenda: A practitioner's perspective. *Corporate Governance: An International Review*, *1*(1), pp.26-32.

Hoanca, B. and Mock, K.J., 2020. Artificial intelligence-based cybercrime. In Encyclopedia of criminal activities and the deep web (pp. 36-51). IGI Global.

Hofer, C.W. (1975) ‘Toward a Contingency Theory of Business Strategy’, *Academy of Management Journal,* 18(4), pp. 784–810. Available at: https://doi.org/10.5465/255379.

Holloway, I. and Wheeler, S., 1996. *Qualitative research for nurses* (pp. p115-129). Oxford: Blackwell Science.

Hsu, L. C. and Wang, C. H. (2012). Clarifying the Effect of Intellectual Capital on Performance: The Mediating Role of Dynamic Capability. British Journal of Management, 23(2), 179–205. https://doi.org/10.1111/j.1467-8551.2010.00718.x

Hu, M., 2020. Cambridge Analytica’s black box. *Big Data & Society*, *7*(2), p.2053951720938091.

Huang, K.F. *et al.* (2015) ‘From Temporary Competitive Advantage to Sustainable Competitive Advantage’, *British Journal of Management,* 26(4), pp. 617–636. Available at: https://doi.org/10.1111/1467-8551.12104.

Hubbard, T., klimavicz, J. F., Wong, S., and Steinhoff, J. C. (2021). Zero Trust in a Virtual Cybersecurity World. Journal of Government Financial Management, 13–24.

Hulland, J. and Wade, M. (2004) ‘The Resource-Based View and Information Systems Research: Review, Extension, and Suggestions for Future Research’, *MIS Quarterly: Management Information Systems*, 28(1), pp. 107–142.

Hung, H. (1998) ‘A typology of the theories of the roles of governing boards’, *Corporate Governance An International Review* ·, 6(February 1998), pp. 101–111. Available at: https://doi.org/10.1111/1467-8683.00089.

Hutchins, S. and Britt, S., 2020. Cybersecurity policies for remote work. *Risk Management*, *67*(9), pp.10-12.

Ingram, P. and Simons, T., 1995. Institutional and resource dependence determinants of responsiveness to work-family issues. *Academy of Management Journal*, *38*(5), pp.1466-1482.

IT Governance Institute. (2003). Board briefing for IT governance, 2nd edition. Rolling Meadows. Re-trieved from https://www.oecd.org/site/ictworkshops/year/2006/37599342.pdf

Itami, H. (1987) ‘6 - Resource Fit’, in *Mobilizing Invisible Assets*. Harvard University Press. Available at: http://ebookcentral.proquest.com/lib/reading/detail.action?docID=3300704.

Izadi, Hossein, B.U. (2017) ‘Strategy Formulation and Firms’ Performance - The Case of High-tech SMEs in the UK’, *Library Technology Reports*, 53(5), pp. 5–11.

Jacobsen, R., 1988. The persistence of abnormal returns. *Strategic management journal*, *9*(5), pp.415-430.

Jansen, K.J. and Shipp, A.J. (2019) ‘Fitting as a Temporal Sensemaking Process: Shifting trajectories and Stable themes’, *Human Relations*, 72(7), pp. 1154–1186. Available at: https://doi.org/10.1177/0018726718794268.

Jazri, H., Zakaria, O., and Chikohora, E. (2018). Measuring Cybersecurity Wellness Index of Critical Organisations. IST-Africa.

Jensen, M. and Zajac, E.J. (2004) ‘Corporate elites and corporate strategy: How demographic preferences and structural position shape the scope of the firm’, *Strategic Management Journal*, 25(6), pp. 507–524. Available at: https://doi.org/10.1002/smj.393.

Jensen, M.C., and Meckling, W.H., 1976. Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of financial economics*, *3*(4), pp.305-360.

Jensen, M.C., 1993. The modern industrial revolution, exit, and the failure of internal control systems. *the Journal of Finance*, *48*(3), pp.831-880.

John H Bickley (1959) ‘The Nature of Business Risk’, *The Journal of Insurance*, 25(4), pp. 32–42.

Johnson, J.L., Daily, C.M. and Ellstrand, A.E., 1996. Boards of directors: A review and research agenda. *Journal of management*, *22*(3), pp.409-438.

Johnson, P. and Clark, M., 2006. Mapping the terrain: an overview of business and management research methodologies. *Business and management research methodologies. London: Sage*.

Johnson, R. and Waterfield, J. (2004) ‘Making words count: the value of qualitative research.’, *Physiotherapy Research international*, 9(3), pp. 121–131. Available at: https://doi.org/10.1002/pri.312.

Jonassen, D.H. (1991) ‘Objectivism versus constructivism: Do we need a new philosophical paradigm?’, *Educational Technology Research and Development*, 39(3), pp. 5–14. Available at: https://doi.org/10.1007/BF02296434.

Jones, R.E. and Abdelfattah, K.R. (2020) ‘Virtual Interviews in the Era of COVID-19: A Primer for Applicants’, *Journal of Surgical Education*, 77(4), pp. 733–734. Available at: https://doi.org/10.1016/j.jsurg.2020.03.020.

Judge, W.Q. and Zeithaml, C.P. (1992) ‘Institutional and Strategic Choice Perspectives on Board Involvement in the Strategic Decision Process’, *The Academy of Management Journal*, 35(4), pp. 766–794.

Kahn, R.L. and Cannell, C.F., 1957. The dynamics of interviewing; theory, technique, and cases.

Kakabadse, A. *et al.* (2001) ‘Role and Contribution of Non-Executive Directors’, *Corporate Governance: The international journal of business in society*, 1(1), pp. 4–8. Available at: https://doi.org/10.1108/EUM0000000005455.

Kakabadse, A., Kakabadse, N.K. and Barratt, R. (2006) ‘Chairman and chief executive officer (CEO): That sacred and secret relationship’, *Journal of Management Development*, 25(2), pp. 134–150. Available at: https://doi.org/10.1108/02621710610645126.

Kakabadse, N.K. and Kakabadse, A.P. (2007) ‘Chairman of the board: Demographics effects on role pursuit’, *Journal of Management Development*, 26(2), pp. 169–192. Available at: https://doi.org/10.1108/02621710710726071.

Kakabadse, N.K. and Louchart, E., 2012. Delicate empiricism: an action learning approach to elite interviewing. *Global elites: The opaque nature of transnational policy determination*, pp.286-307.

Kalinich, K., 2017. Treating Cyber Risks—Using Insurance and Finance. *The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities*, pp.143-158.

Kaplan, R.S. and Mikes, A., 2012. Managing risks: a new framework. *Harvard business review*, *90*(6), pp.48-60.

Katila, R., Rosenberger, J.D. and Eisenhardt, K.M., 2008. Swimming with sharks: Technology ventures, defense mechanisms and corporate relationships. *Administrative science quarterly*, *53*(2), pp.295-332.

Katz, D., and Kahn, R.L., 1978. *The social psychology of organizations* (Vol. 2, p. 528). New York: Wiley.

Kauffman, S.A., 1993. *The origins of order: Self-organization and selection in evolution*. Oxford University Press, USA.

Kauffman, S.A., 1995. *At home in the universe: The search for laws of self-organization and complexity*. Oxford University Press, USA.

Keasey, K. and Wright, M., 1993. Issues in corporate accountability and governance: An editorial. *Accounting and business research*, *23*(sup1), pp.291-303.

Keay, A. (2017) ‘Stewardship theory: is board accountability necessary ?’, *International Journal of Law and Management*, 59(6), pp. 1292–1314. Available at: https://doi.org/10.1108/IJLMA-11-2016-0118.

Ketokivi, M. and Mantere, S. (2010) ‘Two strategies for inductive reasoning in organizational research’, *Academy of Management Review*, 35(2), pp. 315–333. Available at: https://doi.org/10.5465/AMR.2010.48463336.

Kewell, B. (2007) 'Linking Risk and Reputation: A Research Agenda and Methodological Analysis', *Risk Management*, 9(4), pp. 238–254. Available at: https://doi.org/10.1057/palgrave.rm.8250029.

Kiel, G.C. and Kawamoto, C., 1997, September. A conceptual model of strategic management. In *British Academy of Management Annual Conference, London* (pp. 8-10).

Kiesow Cortez E. and Dekker, M. (2022). A Corporate Governance Approach to Cybersecurity Risk Disclosure. European Journal of Risk Regulation, 13(3), 443–463. https://doi.org/10.1017/err.2022.10

King, N., 2004. 21——using templates in the thematic analysis of text——. *Essential guide to qualitative methods in organizational research, 256*.

Kiss, M., Breda, G. and Muha, L. (2019) 'Information security aspects of Industry 4.0', *Procedia Manufacturing*, 32, pp. 848–855. Available at: https://doi.org/10.1016/j.promfg.2019.02.293.

Klein, B., Crawford, R.G. and Alchian, A.A., 1978. Vertical integration, appropriable rents, and the competitive contracting process. *The journal of Law and Economics*, *21*(2), pp.297-326.

Klein, B., Crawford, R.G. and Alchian, A.A., 1978. Vertical integration, appropriable rents, and the competitive contracting process. *The journal of Law and Economics*, *21*(2), pp.297-326.

Klinke, A. and Renn, O. (2006) 'Systemic Risks as Challenge for Policy Making in Risk Governance', *Qualitative Social Research*, 7(1). Available at: http://www.qualitative-research.net/fqs/.

Knights, D. and Morgan, G. (1991) 'Corporate Strategy, Organizations, and Subjectivity: A Critique', *Organization Studies*, 12(2), pp. 251–273. Available at: https://doi.org/10.1177/017084069101200205.

Kogut, B. and Zander, U., 1992. Knowledge of the firm, combinative capabilities, and the replication of technology. *Organization science*, *3*(3), pp.383-397.

Kosnik, R.D., 1987. Greenmail: A study of board performance in corporate governance. *Administrative science quarterly*, pp.163-185.

Kosutic, D. and Pigni, F. (2020a) ‘Cybersecurity: Investing for competitive outcomes’, *Journal of Business Strategy* [Preprint]. Available at: https://doi.org/10.1108/JBS-06-2020-0116.

Kosutic, D. and Pigni, F. (2020b) ‘Investing in cybersecurity: Gaining a competitive advantage through cybersecurity’, *Strategic Direction*, 37(2), pp. 19–21. Available at: https://doi.org/10.1108/SD-11-2020-0205.

Kosutic, D. and Pigni, F. (2020). Cybersecurity: Investing for competitive outcomes. Journal of Business Strategy. https://doi.org/10.1108/JBS-06-2020-0116

Kotz, R.F. (1998) ‘Technology company boards: a new model’, *Directors & Boards*, 22(3).

Kruth, J.G. (2015) ‘Five qualitative research approaches and their applications in parapsychology’, *Journal of Parapsychology*, 79(2), pp. 219–233.

Krutilla, K., Alexeev, A., Jardine, E., and Good, D. (2021). The Benefits and Costs of Cybersecurity Risk Reduction: A Dynamic Extension of the Gordon and Loeb Model. Risk Analysis, 41(10), 1795–1808. https://doi.org/10.1111/risa.13713

Kula, V. and Tatoglu, E., 2006. Board process attributes and company performance of family-owned businesses in Turkey. *Corporate Governance: The international journal of business in society*.

Kure, H.I., Islam, S. and Razzaque, M.A. (2018) ‘An integrated cyber security risk management approach for a cyber-physical system’, *Applied Sciences (Switzerland)*, 8(6). Available at: https://doi.org/10.3390/app8060898.

Landefeld, S., Mejia, L., Handy, A., and Hinnen, T. (2017). ’Is_That_a_Target_on_Your_Back. Corporate Governance Advisor, 25(6), 1–9.

Landefeld, S.M., Mejia, L.R. and Handy, A.C. (2015) ‘Board Tools for Oversight of Cybersecurity Risk’, *The Corporate Governance Advisor*, 23(3), pp. 1–9.

Langø, H.I.G., 2013. Slaying cyber dragons: Competing academic approaches to cyber security.

Lauenstein, M., 1982. Handling the Key Issues. *Journal of Business Strategy*, *2*(4), pp.110-114.

Lavie, D., 2006. The competitive advantage of interconnected firms: An extension of the resource-based view. *Academy of management review*, *31*(3), pp.638-658.

Lee, P.M. and O'Neill, H.M., 2003. Ownership structures and R&D investments of US and Japanese firms: Agency and stewardship perspectives. *Academy of management Journal*, *46*(2), pp.212-225.

Leech, T.J. and Hanlon, L.C. (2017) 'Board Cyber risk Oversight - What needs to change?', in *The Cyber risk handbook*. Available at: http://ebookcentral.proquest.com/lib/reading/detail.action?docID=4837509.

Leibold, M., Probst, G.J. and Gibbert, M., 2007. *Strategic management in the knowledge economy: new approaches and business applications*. John Wiley & Sons.

Leonhardt, F. and Wiedemann, A. (2015) 'Realigning Risk Management in the Light of Industry 4.0', *SSRN Electronic Journal*, pp. 1–22. Available at: https://doi.org/10.2139/ssrn.2678947.

Levi, M. and Leighton Williams, M., 2013. Multi-agency partnerships in cybercrime reduction: Mapping the UK information assurance network cooperation space. *Information Management & Computer Security, 21*(5), pp.420-443.

Lewi, J. and Ritchie, J. (2003) 'Qualitative Research Practice', *Sage Publications,* p. 379.

Li, H., No, W.G. and Wang, T., 2018. SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. *International Journal of Accounting Information Systems*, *30*, pp.40-55.

Lietz, C.A. and Zayas, L.E. (2010) 'Evaluating Qualitative Research for Social Work Practitioners', *Advances in Social Work,* 11(2), pp. 188–202. Available at: https://doi.org/10.18060/589.

Lincoln, Y.S. and Guba, E.G. (2007) 'Judging interpretations: But is it rigorous? Trustworthiness and authenticity in naturalistic evaluation,' *New Directions for Evaluation,* 2007(114), pp. 11–25. Available at: https://doi.org/10.1002/ev.223.

Lincoln, Y.S. and Guba, E.G., 1985. *Naturalistic inquiry*. sage.

Lobschat, L. *et al.* (2021a) ‘Corporate digital responsibility’, *Journal of Business Research*, 122, pp. 875–888. Available at: https://doi.org/10.1016/j.jbusres.2019.10.006.

Lobschat, L. *et al.* (2021b) ‘Corporate digital responsibility’, *Journal of Business Research*, 122, pp. 875–888. Available at: https://doi.org/10.1016/j.jbusres.2019.10.006.

Lobschat, L., Mueller, B., Eggers, F., Brandimarte, L., Diefenbach, S., Kroschke, M., and Wirtz, J. (2021). Corporate digital responsibility. Journal of Business Research, 122, 875–888. https://doi.org/10.1016/j.jbusres.2019.10.006

Loch, K.D., Carr, H.H. and Warkentin, M.E., 1992. Threats to information systems: today's reality, yesterday's understanding. *Mis Quarterly*, pp.173-186.

Lorange, P., 1980. *Corporate planning: An executive viewpoint*. Prentice Hall.

Lorsch, J. and Palepu, K., 2003. Limits to board effectiveness. *Boston, MA: Working Papers. Harvard Business School*.

Lorsch, J.W., 1989. *Pawns or potentates*. Harvard Business School.

Lunn, B. (2014) ‘Strengthened Director Duties of Care for Cybersecurity Oversight Evolving Expectations of Existing Legal Doctrine’, *Journal of Law & Cyber Warfare*, 4(1), pp. 109–137. Available at: https://about.jstor.org/terms.

Lynch, J.M., 1979. *Activating the board of directors: A study of the process of increasing board effectiveness*. Harvard University.

Ma, H. (2006) ‘Competitive advantage: Competitive advantage is not performance’, *Competitiveness Review: An International Business Journal*, 10(2), pp. 15–33.

Mace, M.L., 1971. Directors: Myth and reality.

Machold, S., Huse, M., Minichilli, A. and Nordqvist, M., 2011. Board leadership and strategy involvement in small firms: A team production approach. *Corporate Governance: An International Review*, *19*(4), pp.368-383.

Macintosh, J.C.C. (1999) ‘The issues, effects and consequences of the Berle- Dodd debate, 1931- 1932’, 24, pp. 139–153.

MacLean, L.M., Meyer, M. and Estable, A., 2004. Improving accuracy of transcripts in qualitative research. *Qualitative health research*, *14*(1), pp.113-123.

Mahoney, J.T. and Kor, Y.Y., 2015. Advancing the human capital perspective on value creation by joining capabilities and governance approaches. *Academy of Management Perspectives*, *29*(3), pp.296-308.

Majd, S. and Pindyck, R.S., 1987. The learning curve and optimal production under uncertainty.

Makadok, R. (2001) 'Toward a synthesis of the resource-based and dynamic-capability views of rent creation', *Strategic Management Journal*, 22(5), pp. 387–401. Available at: https://doi.org/10.1002/smj.158.

Makadok, R., 2003. Doing the right thing and knowing the right thing to do: Why the whole is greater than the sum of the parts. *Strategic Management Journal*, *24*(10), pp.1043-1055.

Malecki, F., 2020. Overcoming the security risks of remote working. *Computer fraud & security*, *2020*(7), pp.10-12.

Maleh, Y., Sahid, A. and Belaissaoui, M. (2021) 'A Maturity Framework for Cybersecurity Governance in Organisations', *The EDP Audit, Control, and Security Newsletter (EDPACS)*, 63(6), pp. 1–22. Available at: https://doi.org/10.1080/07366981.2020.1815354.

Malterud, K., 2001. Qualitative research: standards, challenges, and guidelines. *The lancet*, *358*(9280), pp.483-488.

Mandiant (2015). *M-Trends 2015: A View from the Front Lines.* https://www.mandiant.com/resources/reports (Accessed: 13th May 2020)

Manz, C.C., 1986. Self-leadership: Toward an expanded theory of self-influence processes in organizations. *Academy of Management review*, *11*(3), pp.585-600.

Marie L'Huillier, B. (2014) 'What does "corporate governance" actually mean?', *Corporate Governance (Bingley)*, 14(3), pp. 300–319. Available at: https://doi.org/10.1108/CG-10-2012-0073.

Marshall, C., 1990. Goodness criteria: Are they objective or judgement calls. *The paradigm dialog*, pp.188-197.

Martin, D.D. and Wilson, J.L. (2005) 'Role Theory', in *Encyclopedia of Social Theory*, pp. 652–655. Available at: https://doi.org/10.4135/9781412952552.

Martin, K., 2015. Ethical issues in the big data industry. *MIS Quarterly Executive*, *14*, p.2.

Mason, E.S. and Mason, E.S. eds., 1959. *The corporation in modern society* (Vol. 86). Cambridge, MA: Harvard University Press.

Mason, R.B. (2007) 'The external environment' s effect on management and strategy: A complexity theory approach', *Management Decision*, 45(1), pp. 10–28. Available at: https://doi.org/10.1108/00251740710718935.

Mata, F. J., Fuerst, W. L., and Barney, J. B. (1995). Information technology and sustained competitive advantage: A resource-based analysis. MIS Quarterly: Management Information Systems, 19(4), 487–504. https://doi.org/10.2307/249630

Matheu, S. N., Hernández-Ramos, J. L., Skarmeta, A. F., and Baldini, G. (2021). A Survey of Cybersecurity Certification for the Internet of Things. In ACM Computing Surveys (Vol. 53, Issue 6). Association for Computing Machinery. https://doi.org/10.1145/3410160

Mayring, P. (2000) 'Qualitative Content Analysis', *IEEE International Symposium on Industrial Electronics*, 1(2).

McCarthy, D.R. (2018) 'Privatizing political authority: Cybersecurity, public-private partnerships, and the reproduction of liberal political order', *Politics and Governance*, 6(2), pp. 5–12. Available at: https://doi.org/10.17645/pag.v6i2.1335.

McCuddy, M.K. and Pirie, W.L., 2007. Spirituality, stewardship, and financial decision-making: Toward a theory of intertemporal stewardship. *Managerial Finance*, *33*(12), pp.957-969.

McElwee, M., 1998, July. Chaos theory and complexity as fountainheads for design of an organization theory building workshop. In *XIVth World Congress of the International Sociological Association, Montreal, Canada, July*.

McGrath, R.G., and MacMillan, I.C., 2000. *The entrepreneurial mindset: Strategies for continuously creating opportunity in an age of uncertainty* (Vol. 284). Harvard Business Press.

McGrath, R.G., Ferrier, W.J. and Mendelow, A.L. (2004) 'Real options as engines of choice and heterogeneity', *Academy of Management Review*, 29(1), pp. 86–101. Available at: https://doi.org/10.5465/AMR.2004.11851720.

McGregor, D., 1960. Theory X and theory Y. *Organization theory*, *358*(374), p.5.

McKinley, S.K. *et al.* (2020) 'Successful Virtual Interviews: Perspectives from Recent Surgical Fellowship Applicants and Advice for Both Applicants and Programs', *Annals of surgery*, 272(2), pp. e192–e196. Available at: https://doi.org/10.1097/SLA.0000000000004172.

McLellan, E., MaCqueen, K.M. and Neidig, J.L. (2003) 'Beyond the Qualitative Interview: Data Preparation and Transcription', *Field Methods*, 15(1), pp. 63–84. Available at: https://doi.org/10.1177/1525822X02239573.

McNulty, T. and Pettigrew, A. (1999) 'Strategists on the Board', *Organisation Studies*, 21(1), pp. 47–74. Available at: https://doi.org/0803973233.

McNulty, T., Zattoni, A. and Douglas, T., 2013. Developing corporate governance research through qualitative methods: A review of previous studies. *Corporate Governance: An International Review*, *21*(2), pp.183-198.

Meyer, J.W. and Rowan, B., 1977. Institutionalized organizations: Formal structure as myth and ceremony. *American journal of sociology*, *83*(2), pp.340-363.

Meyer, J.W. and Scott, W.R., 1983. *Organizations and environments: Ritual and rationality*. Beverly Hills, CA: SAGE.

Meyer, S.B. and Lunnay, B. (2013) 'The application of abductive and retroductive inference for the design and analysis of theory-driven sociological research', *Sociological Research Online*. Available at: https://doi.org/10.5153/sro.2819.

Michael, K., Kobran, S., Abbas, R., and Hamdoun, S. (2019). Privacy, Data Right and Cybersecurity. IEEE International Symposium on Technology in Society.

Mikecz, R. (2012) 'Interviewing Elites: Addressing Methodological Issues', *Qualitative Inquiry*, 18(6), pp. 482–493. Available at: https://doi.org/10.1177/1077800412442818.

Miles, M.B. and Huberman, A.M., 1994. *Qualitative data analysis: An expanded sourcebook*. sage.

Miller, J., 2000. Millennium intelligence: understanding and conducting competitive intelligence in the digital age. Information Today, Inc..

Miller, A.D. and Oldroyd, D. (2018) 'Does Stewardship Still Have a Role?', *Accounting Historians Journal*, 45(1), pp. 69–82. Available at: https://doi.org/10.2308/aahj-10585.

Minichilli, A. and Hansen, C., 2007. The board advisory tasks in small firms and the event of crises. *Journal of management & governance*, *11*, pp.5-22.

Ministry of Defence, 2016. Development, Concepts and Doctrine Centre, "Cyber primer (second edition)," Joint Doctrine Publication [Technical Report], https://www.gov.uk/government/publications/cyber-primer.

Mintzberg, H., 1978. Patterns in strategy formation. *Management science*, *24*(9), pp.934-948.

Mintzberg, H., 1983. Power in and around organizations.

Mintzberg, H., et al., (1998) Strategy Safari: A Guided Tour through the Wilds of Strategic Management. Prentice Hall, Upper Saddle River.

Mishra, S., 2023. Exploring the Impact of AI-Based Cyber Security Financial Sector Management. Applied Sciences, 13(10), p.5875.

Mitnick, B. (2019) 'GUIDEPOST: The Theory of Agency Redux', *Academy of Management Discoveries* [Preprint]. Available at: https://doi.org/10.5465/amd.2019.0136.

Mittman, B.S., 2001, November. Qualitative methods and rigorous management research:(How) are they compatible. In White paper prepared for the Department of Veterans Affairs Management Research in VA Workshop, sponsored by the HSR&D Management Decision and Research Center (Vol. 11, pp. 19-20).

Mizruchi, M.S. (1983) 'Who Controls Whom? An Examination of the Relation between Management and Boards of Directors in Large American Corporations,' *The Academy of Management Review*, 8(3), pp. 426–435. Available at: https://www.jstor.org/stable/257831.

Montgomery, C.A. and Collis, D., 1995. Competing on resources: strategy in the 1990s. *Harvard Business Review*, *73*(4), pp.118-128.

Moore, A.P., Cappelli, D.M. and Trzeciak, R.F., 2008. The "big picture" of insider IT sabotage across US critical infrastructures (pp. 17-52). Springer US.

Moore, T., Dynes, S., and Chang, F.R. (2015) ‘Identifying How Firms Manage Cybersecurity Investment’, *Workshop on the Economics of Information Security (WEIS), Berkeley, CA*, pp. 1–27.

Morrison, A. and Kumar, G. (2018). Corporate Boards May Be More Likely Than Regulators to Scrutinize Cybersecurity Program Effectiveness This Year. Journal of Health Care Compliance, 49–54.

Morrow, S.L. (2007) ‘Qualitative Research in Counseling Psychology: Conceptual Foundations’, *The Counseling Psychologist*, 35(2), pp. 209–235. Available at: https://doi.org/10.1177/0011000006286990.

Möslein, F. (2018) ‘Robots in the Boardroom: Artificial Intelligence and Corporate Law’, in W. Barfield and U. Pagallo (eds) *Research Handbook on the Law of Artificial Intelligence*, pp. 649–670.

Moustakas, C., 1994. *Phenomenological research methods*. Sage publications.

Mowlana, H., 1997. *Global information and world communication: new frontiers in international relations*. Sage.

Mulligan, D. K. and Schneider, F. B. (2011). Doctrine for cybersecurity. Daedalus, 140(4), 70–92. https://doi.org/10.1162/DAED_a_00116

Muth, M. and Donaldson, L., 1998. Stewardship theory and board structure: A contingency approach. *Corporate Governance: An International Review*, *6*(1), pp.5-28.

Nader, R., 1984. Reforming corporate governance. *California Management Review (pre-1986)*, *26*(000004), p.126.

Nadler, D.A. (2004) ‘What’s the board’s role in strategy development? Engaging the board in corporate strategy,’ *Strategy & Leadership*, 32(5), pp. 25–33. Available at: https://doi.org/10.1108/10878570410557633.

Nagy, J. *et al.* (2018) ‘The role and impact of industry 4.0 and the internet of things on the business strategy of the value chain-the case of hungary’, *Sustainability (Switzerland)*, 10(10). Available at: https://doi.org/10.3390/su10103491.

Nahapiet, J. and Ghoshal, S., 1998. Social capital, intellectual capital, and the organizational advantage. *Academy of management review*, *23*(2), pp.242-266.

Nasution, M.K.M. (2018) 'Ontology', *Journal of Physics: Conference Series*, 1116(2). Available at: https://doi.org/10.1088/1742-6596/1116/2/022030.

Nelson, R.R., and Winter, S.G., 1982. The Schumpeterian tradeoff revisited. *The American Economic Review*, *72*(1), pp.114-132.

Nicholls, J., Kuppa, A., and Le-Khac, N.A. (2021) 'Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape', *IEEE Access*, 9, pp. 163965–163986. Available at: https://doi.org/10.1109/ACCESS.2021.3134076.

Nicholson, G. and Cameron, N. (2010) 'The Role of the Board of Directors: Perception of Managerial Elites', *Journal of Management and Organisation*, 16(February), pp. 204–218.

Nielsen, K. (2007) 'The qualitative research interview and issues of knowledge', *Nordic Psychology*, 59(3), pp. 210–222. Available at: https://doi.org/10.1027/1901-2276.59.3.210.

Noda, T., and Bower, J.L., 1996. Strategy making as iterated processes of resource allocation. *Strategic management journal*, *17*(S1), pp.159-192.

Nodeland, B., Belshaw, S. and Saber, M. (2019) 'Teaching Cybersecurity to Criminal Justice Majors', *Journal of Criminal Justice Education*, 30(1), pp. 71–90. Available at: https://doi.org/10.1080/10511253.2018.1439513.

Nolan, C., Lawyer, G., and Dodd, R.M. (2019) 'Cybersecurity: today's most pressing governance issue', *Journal of Cyber Policy*, 4(3), pp. 425–441. Available at: https://doi.org/10.1080/23738871.2019.1673458.

Nowell, L.S. *et al.* (2017) 'Thematic Analysis: Striving to Meet the Trustworthiness Criteria', *International Journal of Qualitative Methods*, 16, pp. 1–13. Available at: https://doi.org/10.1177/1609406917733847.

Ochieng, P.A. (2009) 'An Analysis of the Strengths and Limitation of Qualitative and Quantitative Research Paradigms', *Problems of Education in the 21st Century*, 13, pp. 1–18.

OECD, O., 2004. The OECD principles of corporate governance. *Contaduría y Administración*, (216).

Ogbanufe, O., Crossler, R. E., and Biros, D. (2021). Exploring stewardship: A precursor to voluntary security behaviors. Computers and Security, 109. https://doi.org/10.1016/j.cose.2021.102397

Oldroyd, D. and Miller, A.D., 2011. In defense of stewardship. *The CPA Journal*, *81*(10), p.6.

Oliver, C. (1997) 'Sustainable Competitive Advantage: Combining Institutional and Resource-Based Views', *Management Journal*, 18(9), pp. 697–713. Available at: https://www.jstor.org/stable/3088134?seq=1&cid=pdf-.

Oliver, R.W. (2000) 'The Board's Role: Driver's Seat or Rubber Stamp?', *Journal of Business Strategy*, 21(4), pp. 7–9.

Onwuegbuzie, A.J., Leech, N.L. and Collins, K.M.T. (2010) 'Innovative data collection strategies in qualitative research', *The Qualitative Report*, 15(3), pp. 696–726.

Padgett, D.K., 2008. *Qualitative methods in social work research* (Vol. 20). Sage publications.

Palmer, D., 1983. Broken ties: Interlocking directorates and intercorporate coordination. *Administrative science quarterly*, pp.40-55.

Parent, M., and Reich, B.H. (2009) 'Governing Information Technology Risk', *California Management Review*, 51(3).

Parker, D.B., 1998. *Fighting computer crime: A new framework for protecting information*. John Wiley & Sons, Inc.

Parmar, B.L. *et al.* (2010) 'Stakeholder Theory: The State of the Art', *The Academy of Management Annals*, 4(1), pp. 1–61. Available at: https://doi.org/10.1080/19416520.2010.495581.

Patton, M.Q. (2002) 'Two Decades of Developments in Qualitative Inquiry: A Personal, Experiential Perspective', *Qualitative Social Work*, 1(3), pp. 261–283.

Pavlou, P.A. and Sawy, O.A.E. (2010) 'The "third hand": IT-enabled competitive advantage in turbulence through improvisational capabilities', *Information Systems Research*, 21(3), pp. 443–471. Available at: https://doi.org/10.1287/isre.1100.0280.

Peng, S.Y. (2018) '"Private" cybersecurity standards? Cyberspace Governance, Multistakeholderism, and the (Ir)relevance of the TBT Regime,' *Cornell International Law Journal*, 51(2), pp. 445–469.

Pennings, J.M., 1980. *Interlocking directorates: Origins and consequences of connections among organizations' Board of Directors*. Jossey-Bass.

Perrons, R.K. and Jensen, J.W., 2015. Data as an asset: What the oil and gas sector can learn from other industries about "Big Data." *Energy Policy*, *81*, pp.117-121.

Peteraf, M. A. (1993). The Cornerstones of Competitive Advantage: A Resource-Based View. Strategic Management Journal, 14(3), 179–191. https://doi.org/10.1002/smj.4250140303

Peteraf, M.A. and Bergen, M.E. (2003) 'Scanning dynamic competitive landscapes: A market-based and resource-based framework', *Strategic Management Journal*, 24(10 SPEC ISS.), pp. 1027–1041. Available at: https://doi.org/10.1002/smj.325.

Pettigrew, A.M., 1992. On studying managerial elites. *Strategic management journal*, *13*(S2), pp.163-182.

Petty, N.J., Thomson, O.P. and Stew, G. (2012) 'Ready for a paradigm shift? Part 1: Introducing the philosophy of qualitative research', *Manual Therapy*, 17(4), pp. 267–274. Available at: https://doi.org/10.1016/j.math.2012.03.006.

Pfeffer, J. and Salancik, G. R., 1978. *The External Control of Organizations: A Resource Dependence Perspective.* Stanford University Press.

Phillips, N., Hardy, C. (2002): Discourse Analysis: Investigating Processes of Social Construction. *Qualitative research methods series*, *50.*

Piccarozzi, M., Aquilani, B. and Gatti, C. (2018) 'Industry 4.0 in management studies: A systematic literature review', *Sustainability (Switzerland)*, 10(10), pp. 1–24. Available at: https://doi.org/10.3390/su10103821.

Ponterotto, J.G. (2005) 'Qualitative research in counseling psychology: A primer on research paradigms and philosophy of science', *Journal of Counseling Psychology*, 52(2), pp. 126–136. Available at: https://doi.org/10.1037/0022-0167.52.2.126.

Porter, M.E., 1985. Technology and competitive advantage. *Journal of business strategy*, *5*(3), pp.60-78.

Porter, Michael E. 1980. *Competitive Strategy: Techniques for analyzing industries and competitors.* New York, The Free Press.

Post, G. and Kagan, A., 2000. Management tradeoffs in anti-virus strategies. *Information & Management*, *37*(1), pp.13-24.

Posthumus, S., Von Solms, R. and King, M. (2010) 'The board and IT governance: What, who and how', *South African Journal of Business Management*, 41(3), pp. 23–32.

Pound, J., 1995. The promise of the governed corporation. *Harvard Business Review*, *73*(2), pp.89-98.

Powell, T.C. (2001) 'Competitive advantage: Logical and philosophical considerations', *Strategic Management Journal*, 22(9), pp. 875–888. Available at: https://doi.org/10.1002/smj.173.

Prahalad, C.K. and Hamel, G. (1990) 'The Core Competence of the Corporation', *Harvard Business Review*. Available at: www.hbr.org.

Pranggono, B. and Arabo, A. (2021) 'COVID -19 pandemic cybersecurity issues ', *Internet Technology Letters*, 4(2). Available at: https://doi.org/10.1002/itl2.247.

Premium Official News. (2022). How to leverage cybersecurity to gain customer trust. Right Vision Media.

Preston, L.E. and Sapienza, H.J., 1990. Stakeholder management and corporate performance. *Journal of behavioral Economics*, *19*(4), pp.361-375.

Price, J.H. and Murnan, J. (2004) 'Research Limitations and the Necessity of Reporting Them', *American Journal of Health Education*, 35(2), pp. 66–67.

Priem, R.L. and Butler, J.E. (2001) 'Is the Resource-Based "View" a Useful Perspective for Strategic Management Research?', *The Academy of Management Review*, 26(1), p. 22. Available at: https://doi.org/10.2307/259392.

Radanliev, P. *et al.* (2019) 'Cyber Security Framework for the Internet-of-Things in Industry 4. 0', *Munich Personal RePEc Archive*, (March), pp. 1–7. Available at: https://doi.org/10.20944/preprints201903.0111.v1.

Rai, M. and Mandoria, H.L. (2019) 'A Study on Cyber Crimes, Cyber Criminals and Major Security Breaches', *International Research Journal of Engineering and Technology*, 6(07), p. 233. Available at: www.irjet.net.

Rai, M. and Mandoria, H. L. (2019). A Study on Cyber Crimes, Cyber Criminals and Major Security Breaches. International Research Journal of Engineering and Technology, 6(07), 233. www.irjet.net

Randøy, T. and Nielsen, J., 2002. Company performance, corporate governance, and CEO compensation in Norway and Sweden. *Journal of Management and Governance*, *6*, pp.57-81.

Rechner, P.L., 1989. Corporate governance: fact or fiction? *Business Horizons*, *32*(4), pp.11-16.

Reed, R. and DeFillippi, R.J., 1990. Causal ambiguity, barriers to imitation, and sustainable competitive advantage. *Academy of management review*, *15*(1), pp.88-102.

Rhodes, D., Rechner, P. and Sundaramurthy, C., 2001. A Meta-Analysis of Board Leadership Structure, Financial Performance: Are Two Heads Better Then One. *Corporate Governance: An International Review*, *9*(4), pp.311-319.

Ricardo, David. 1817. *On the Principles of Political Economy and Taxation.* Available online at the Library of Economics and Liberty: http://www .econlib.org/library/Ricardo/ricP.html.

Rindova, V.P. (1999) 'What corporate boards have to do with strategy: A cognitive perspective', *Journal of Management Studies*, 36(7), pp. 953–975. Available at: https://doi.org/10.1111/1467-6486.00165.

Rindova, V.P., Williamson, I.O. and Petkova, A.P. (2010) 'Reputation as an intangible asset: Reflections on theory and methods in two empirical studies of business school reputations', *Journal of Management*, 36(3), pp. 610–619. Available at: https://doi.org/10.1177/0149206309343208.

Roberts, K., and Weitzman, M.L., 1981. Funding criteria for research, development, and exploration projects. *Econometrica: Journal of the Econometric Society*, pp.1261-1288.

Ross, R. and Bryan, S. (2022) 'Your_Guide_to_Cyberspace_Comm', *Arlington Army*, 72(12), pp. 34–38.

Roundtable, 1990. Corporate Governance and American Competitiveness. *BuS. LaW.*, *46*, pp.241-244.

Rowan, B., 1982. Organizational structure and the institutional environment: The case of public schools. *Administrative science quarterly*, pp.259-279.

Rumelt, R.P., 1984. Towards a strategic theory of the firm. *Competitive strategic management*, *26*(3), pp.556-570.

Ryan, G.W. and Bernard, H.R., 2000. Techniques to identify themes in qualitative data.

Sallos, M. P., Garcia-Perez, A., Bedford, D., and Orlando, B. (2019). Strategy and organisational cybersecurity: a knowledge-problem perspective. Journal of Intellectual Capital, 20(4), 581–597. https://doi.org/10.1108/JIC-03-2019-0041

Sandelowski, M. and Barroso, J., 2002. Reading qualitative studies. *International journal of qualitative methods*, *1*(1), pp.74-108.

Saunders, M., Lewis, P. and Thornhill, A. (2009a) *Research Methods for Business Students*.

Saunders, M., Lewis, P. and Thornhill, A. (2009b) 'Understanding research philosophies and...', in, pp. 122–161.

Schillemans, T. and Bjurstrøm, K.H. (2019) 'Trust and Verification: Balancing Agency and Stewardship Theory in the Governance of Agencies', *International Public Management Journal*, 0(0), pp. 1–35. Available at: https://doi.org/10.1080/10967494.2018.1553807.

Schroeder, A. *et al.* (2019) 'Capturing the benefits of industry 4.0: a business network perspective', *Production Planning and Control*, 30(16), pp. 1305–1321. Available at: https://doi.org/10.1080/09537287.2019.1612111.

Schwab, W. and Poujol, M. (2018) 'The State of Industrial Cybersecurity 2018', *Kaspersky Lab*, (June), p. 23.

Schwandt, T.A., Lincoln, Y.S. and Guba, E.G., 2007. Judging interpretations: But is it rigorous? Trustworthiness and authenticity in naturalistic evaluation. *New directions for evaluation*, *2007*(114), pp.11-25.

Sellevol, T., Huse, M. and Hansen, C., 2007. Research Report „The Value Creating Board ". *Norwegian School of Management*.

Selznick, P., 1957. Law and the Structures of Social Action.

Selznick, P., 1996. Institutionalism" old" and" new". *Administrative science quarterly*, pp.270-277.

Shackelford, S.J., Fort, T.L. and Charoen, D. (2016) 'Sustainable cybersecurity: Applying lessons from the green movement to managing cyber attacks', *University of Illinois Law Review*, 2016(5), pp. 1995–2032. Available at: https://doi.org/10.2139/ssrn.2324620.

Shen, W. (2003) 'The dynamics of the CEO-board relationship: An evolutionary perspective', *Academy of Management Review*, 28(3), pp. 466–476. Available at: https://doi.org/10.5465/AMR.2003.10196776.

Shen, W. and Cannella Jr, A.A., 2002. Revisiting the performance consequences of CEO succession: The impacts of successor type, post-succession senior executive turnover, and departing CEO tenure. *Academy of management journal*, *45*(4), pp.717-733.

Shenton, A.K. (2004) 'Strategies for ensuring trustworthiness in qualitative research projects', *Education for Information*, 22, pp. 63–75.

Shong, Y.T. (2019) 'Achieving cybersecurity can yield a competitive advantage', *The Business Times, Singapore*, pp. 1–3.

Sim, J. and Wright, C., 2000. *Research in health care: concepts, designs, and methods*. Nelson Thornes.

Sison, L.V. and Kleiner, B.H., 2001. Differences between company officers and company executives. *Management Research News*, *24*(3/4), pp.157-161.

Sitkin, S.B., 1992. Learning through failure: The strategy of small losses. *Research in organizational behavior*, *14*, pp.231-266.

Sluss, D.M., Dick, R. van and Thompson, B. (2013) 'Role Theory in Organisations: A Relational Perspective', *Handbook of I/O-Psychology*, 53(9). Available at: https://doi.org/10.1017/CBO9781107415324.004.

Slywotzky, A.J. and Drzik, J., 2005. Countering the biggest risk of all. *Harvard Business Review*, *83*(4), pp.78-88.

Snape, D. and Spencer, L., 2003. The foundations of qualitative research'in Ritchie, J. and Lewis, J (eds) Qualitative Research Practice.

Snell, S.A., and Dean Jr, J.W., 1992. Integrated manufacturing and human resource management: A human capital perspective. *Academy of Management journal*, *35*(3), pp.467-504.

Souster, R. (2014) 'Corporate Governance: The Board of Directors and Standing Committees', *ACCA*, pp. 1–9. Available at: https://doi.org/10.2470/rflr.v9.n1.1.

Starik, M., 1995. Should trees have managerial standing? Toward stakeholder status for non-human nature. Journal of business ethics, 14, pp.207-217.

Steiner, G.A., 1979. Contingency theories of strategy and strategic management. *Strategic management: A new view of business policy and planning*, pp.405-416.

Stevens, T. (2018) 'Global cybersecurity: new directions in theory and methods', *Politics and Governance*, 6(2), pp. 1–4. Available at: https://doi.org/10.17645/pag.v6i2.1569.

Stevens, T. and O'brien, K. (2019) 'Brexit and cyber security', *RUSI Journal*, 164(3), pp. 22–30. Available at: https://doi.org/10.1080/03071847.2019.1643256.

Stiles, P. (2001) 'The impact of the board on strategy: An empirical examination', *Journal of Management Studies*, 38(5), pp. 627–650. Available at: https://doi.org/10.1111/1467-6486.00252.

Stiles, P. and Taylor, B., 2001. *Boards at work: How directors view their roles and responsibilities: How directors view their roles and responsibilities*. OUP Oxford.

Stinchcombe, A., 1965. Organization-creating organizations. *Trans-action*, *2*(2), pp.34-35.

Stoddart, K. (2016) 'UK cyber security and critical national infrastructure protection', *International Affairs*, 5, pp. 1079–1105.

Stryker, S., and Burke, P.J., 2000. The past, present, and future of an identity theory. *Social psychology quarterly*, pp.284-297.

Stuart, S. (2019) ‘Spencer Stuart Board Index’.

Sundaramurthy, C. and Lewis, M. (2003) ‘Control and Collaboration: Paradoxes of Governance’, *The Academy of Management Review*, 28(3), pp. 397–415. Available at: https://www.jstor.org/stable/30040729.

Teece, D. J. (2007). Explicating Dynamic Capabilities: The Nature and Microfoundations of Sustainable Enterprise Performance. Strategic Management Journal, 28(August). https://doi.org/10.1002/smj

Teece, D. J., Pisano, G., and Shuen, A. M. Y. (1997). Dynamic Capabilities and Strategic Management. Strategic Management Journal, 18(7), 509–533.

Teeters, A.C., 2007. *Use of a wearable camera system in conversation: Toward a companion tool for social-emotional learning in autism* (Doctoral dissertation, Massachusetts Institute of Technology).

Tengelin, V., 1981. The vulnerability of the computerised society. *Information, communication, and computer policies for the’80s*, pp.205-213.

Thackray, H., McAlaney, J., Dogan, H., Taylor, J., and Richardson, C. (2016). Social psychology: An under-used tool in cybersecurity. Proceedings of the 30th International BCS Human Computer Interaction Conference, HCI 2016, 2016-July. https://doi.org/10.14236/ewic/HCI2016.64

Thomas, D.R. (2006) ‘A general inductive approach for qualitative data analysis’, *American Journal of Evaluation*, 27(2).

Thomas, M. ed., 2011. *Deconstructing digital natives: young people, technology, and the new literacies*. Taylor & Francis.

Thompson, J. D. (1967). *Organizations in action: Social science bases of administrative theory.* McGraw-Hill.

Thorne, S., 1997. The art (and science) of critiquing. *Completing a qualitative project: Details and dialogue*, pp.117-132.

Tikk-Ringas, E., 2015. *Evolution of the Cyber Domain: The Implications for National and Global Security*. Routledge.

Tisdale, S.M. (2015) ‘Cybersecurity: Challenges from a Systems, Complexity, Knowledge Management and Business Intelligence Perspective’, *Issues in Information Systems*, 16(Iii), pp. 191–198.

Tongco, M.D.C. (2007) ‘Purposive sampling as a tool for informant selection’, *Ethnobotany Research and Applications*, 5, pp. 147–158. Available at: https://doi.org/10.17348/era.5.0.147-158.

Tosun, O.K., 2021. Changes in corporate governance: externally dictated vs voluntarily determined. *International Review of Financial Analysis*, *73*, p.101608.

Toulmin, S.E., 2003. *The uses of argument*. Cambridge university press.

Tracy, S.J., 2010. Qualitative quality: Eight “big tent” criteria for excellent qualitative research. *Qualitative inquiry*, *16*(10), pp.837-851.

Trautman, L. J. (2014). Managing Cyberthreat. SSRN Electronic Journal, 33(2). https://doi.org/10.2139/ssrn.2534119

Trautman, L.J. (2017) ‘Industrial Cyber Vulnerabilities: Lessons from Stuxnet and the Internet of Things’, *SSRN Electronic Journal*, pp. 761–826. Available at: https://doi.org/10.2139/ssrn.2982629.

Trautman, L.J. and Alternbaumer-Price, K. (2011) ‘The Board’s Responsibility for Information Technology Governance’, *John Marshall Journal of Computer & Information Law*, pp. 313–342.

Tricker, R.I., 1994. The board's role in strategy formulation: Some cross-cultural comparisons. *Futures*, *26*(4), pp.403-415.

Trickett, E.J., 1994. Human diversity and community psychology: Where ecology and empowerment meet. *American journal of community psychology*, *22*(4), p.583.

Turner, D.W. (2010) ‘Qualitative interview design: A practical guide for novice investigators’, *Qualitative Report*, 15(3), pp. 754–760.

Turner, R.H., 1962. Role taking: Process versus conformity. *Life as theater: A dramaturgical sourcebook*, pp.85-98.

Tushman, M.L., Virany, B. and Romanelli, E., 1985. *Effects of CEO and executive team succession: A longitudinal analysis*. Columbia university working paper.

Uhl-Bien, M., Marion, R. and McKelvey, B. (2007) 'Complexity Leadership Theory: Shifting leadership from the industrial age to the knowledge era', *Leadership Quarterly*, 18(4), pp. 298–318. Available at: https://doi.org/10.1016/j.leaqua.2007.04.002.

Useem, M. (2003) 'Corporate governance is directors making decisions: Reforming the outward foundations for inside decision making', *Journal of Management and Governance*, 2(1), pp. 241–253. Available at: https://doi.org/10.22495/cocv2i1p10.

Useem, M., 1978. The inner group of the American capitalist class. *Social Problems*, *25*(3), pp.225-240.

Valentine, E.L.H. and Stewart, G. (2013) 'The emerging role of the Board of Directors in enterprise business technology governance', *International Journal of Disclosure and Governance*, 10(4), pp. 346–362. Available at: https://doi.org/10.1057/jdg.2013.11.

Valeriano, B. and Maness, R.C. (2018a) 'How we stopped worrying about cyber doom and started collecting data', *Politics and Governance*, 6(2), pp. 49–60. Available at: https://doi.org/10.17645/pag.v6i2.1368.

Valeriano, B. and Maness, R.C. (2018b) 'International relations theory and cyber security: Threats, conflicts, and ethics in an emergent domain', in *The Oxford Handbook of International Political Theory*, pp. 259–272. Available at: https://doi.org/10.1093/oxfordhb/9780198746928.013.19.

van de Bunt, E., 2016. The effect of the perfect enemy: Anonymous' representation in the news media.

Van den Berghe, L.A. and Levrau, A., 2004. Evaluating boards of directors: what constitutes a good corporate board? *Corporate Governance: an international review*, *12*(4), pp.461-478.

Van Dis, E.A.M. *et al.* (2023) 'ChatGPT: five priorities for research', *Nature*, 614, pp. 224–226.

Van Ees, H., Gabrielsson, J. and Huse, M. (2009) 'Toward a behavioral theory of boards and corporate governance', *Corporate Governance: An International Review*, 17(3), pp. 307–319. Available at: https://doi.org/10.1111/j.1467-8683.2009.00741.x.

Van Puyvelde, S., Caers, R., Du Bois, C. and Jegers, M., 2012. The governance of nonprofit organizations: Integrating agency theory with stakeholder and stewardship theories. *Nonprofit and voluntary sector quarterly*, *41*(3), pp.431-451.

Van Puyvelde, S., Caers, R., Du Bois, C. and Jegers, M., 2012. The governance of nonprofit organizations: Integrating agency theory with stakeholder and stewardship theories. *Nonprofit and voluntary sector quarterly*, *41*(3), pp.431-451.

Vance, S.C., 1968. The Corporate Director: A Critical Evaluation, Homewood, Illinois: Dow-Jones, Irwin.

Vance, S.C., 1983. *Corporate leadership: Boards, directors, and strategy*. McGraw-Hill College.

Varian, H.R., 2014. Big data: new tricks for econometrics. *Journal of Economic Perspectives*, *28*(2), pp.3-28.

Volti, R., 1995. Society and technological change. New York: St.

von Solms, B. and von Solms, R. (2018). Cybersecurity and information security – what goes where? Information and Computer Security, 26(1), 2–9. https://doi.org/10.1108/ICS-04-2017-0025

Waever, O., 1995. Identity, integration, and security: Solving the sovereignty puzzle in EU studies. *Journal of international affairs*, pp.389-431.

Waldrop, M.M., 1993. *Complexity: The emerging science at the edge of order and chaos*. Simon and Schuster.

Walker, D.-M., Ives, J. and Damery, S. (2017) 'Qualitative Data Collection', in *An Introduction to Health Services Research*, pp. 99–114. Available at: https://doi.org/10.4135/9781473920514.n7.

Walters, R., 2015. Cyber-attacks on US companies since November 2014. *The Heritage Foundation*, *4487*.

Wang, H.-L. (2014) 'Theories for Competitive Advantage', in *Being Practical with Theory: A Window into Business Research*, pp. 33–43.

Wasserman, N. (2006) ‘Stewards, agents, and the founder discount: Executive compensation in new ventures’, *Academy of Management Journal*, 49(5), pp. 960–976. Available at: https://doi.org/10.5465/AMJ.2006.22798177.

Watson, C., Husband, G. and Ireland, A. (2020) *Opening the ‘black box’: what does observational research reveal about processes and practices of governing? Journal of Management and Governance*. Springer US. Available at: https://doi.org/10.1007/s10997-020-09503-3.

Watts, R.L. and Zimmerman, J.L., 1979. The demand for and supply of accounting theories: The market for excuses. *Accounting review*, pp.273-305.

Weick, K.E., 1995. *Sensemaking in organizations* (Vol. 3). Sage.

Wernerfelt, B. (1984) ‘A Resource-based View of the Firm’, *Strategic Management Journal*, 5(June 1982), pp. 171–180.

Wessels, M., van den Brink, P., Verburgh, T., Cadet, B., and van Ruijven, T. (2021). Understanding incentives for cybersecurity investments: Development and application of a typology. Digital Business, 1(2), 100014. https://doi.org/10.1016/j.digbus.2021.100014

Westphal, J.D. and Fredrickson, J.W. (2001) ‘Who directs strategic change? Director experience, the selection of new CEOs, and change in corporate strategy,’ *Strategic Management Journal*, 22(12), pp. 1113–1137. Available at: https://doi.org/10.1002/smj.205.

Westphal, J.D. and Stern, I., 2006. The other pathway to the boardroom: Interpersonal influence behavior as a substitute for elite credentials and majority status in obtaining board appointments. *Administrative science quarterly*, *51*(2), pp.169-204.

Westphal, J.D. and Zajac, E.J., 1995. Who shall govern? CEO/board power, demographic similarity, and new director selection. *Administrative science quarterly*, pp.60-83.

Whittemore, R., Chase, S.K. and Mandle, C.L. (2001) ‘Pearls, pith, and provocation: Validity in Qualitative Research’, *Qualitative Health Research*, 11(4), pp. 522–537.

Whittington, G., 1993. Corporate governance and the regulation of financial reporting. *Accounting and Business Research*, *23*(sup1), pp.311-319.

Wiersma, W., 2000. Research methods in education: An introduction. Needham Heights: A.

Wilkins, A.L., 1989. *Developing corporate character: How to successfully change an organization without destroying it*. Jossey-Bass.

Williams MC (2003) Words, images, enemies: Securitization in international politics. International Studies Quarterly 47 (4): 511-531

Willis, A., 2005. Corporate governance and management of information and records. *Records Management Journal*, *15*(2), pp.86-97.

Winter, S.G. (2003) 'Understanding dynamic capabilities', *Strategic Management Journal*, 24(10 SPEC ISS.), pp. 991–995. Available at: https://doi.org/10.1002/smj.318.

Wirth, A. (2020) 'COVID-19 and What It Means for Cybersecurity', *Biomedical Instrumentation and Technology*, 54(3), pp. 216–219. Available at: https://doi.org/10.2345/0899-8205-54.3.216.

Wirtz, J., Kunz, W. H., Hartley, N., and Tarbit, J. (2022). Corporate Digital Responsibility in Service Firms and Their Ecosystems. Journal of Service Research. https://www.researchgate.net/publication/363487796

Wolfram, S., 2002. *A new kind of science* (Vol. 5, p. 130). Champaign: Wolfram media.

Wood, F. and Bloor, M., 2006. Keywords in qualitative methods: A vocabulary of research concepts. *Keywords in Qualitative Methods*, pp.1-208.

World Economic Forum (2022) *The Global Risks Report 2022*. World Economic Forum.

World Economic Forum and Accenture (2023) *Global Cybersecurity Outlook 2023 Contents*. Geneva.

World Economic Forum. (2012). Partnering for Cyber Resilience.

Wright, M. T. (2021). Cybersecurity: The Human Factor. Independent Banker.

Wrzesniewski, A. and Dutton, J.E., 2001. Crafting a job: Revisioning employees as active crafters of their work. *Academy of management review*, *26*(2), pp.179-201.

Yar Hamidi, D. (2016) *Governance for Innovation–Board Leadership and Value Creation in Entrepreneurial Firms*.

Yermack, D. (2017) ‘Corporate governance and blockchains’, *Review of Finance*, 21(1), pp. 7–31. Available at: https://doi.org/10.1093/rof/rfw074.

Yin, R.K., 2003. Designing case studies. *Qualitative research methods*, *5*(14), pp.359-386.

Yurdusev, A.N., 1993. 'Level of Analysis' and'Unit of Analysis': A Case for Distinction. *Millennium*, *22*(1), pp.77-88.

Zahra, S.A. (1990) ‘Increasing the board’s involvement in strategy’, *Long Range Planning*, 23(6), pp. 109–117. Available at: https://doi.org/10.1016/0024-6301(90)90108-G.

Zahra, S.A. and Pearce, J.A. (1990) ‘Determinants of board directors’ strategic involvement’, *European Management Journal*, 8(2), pp. 164–173. Available at: https://doi.org/10.1016/0263-2373(90)90082-H.

Zetter, K., 2015. The NSA acknowledges what we all feared: Iran learns from US Cyberattacks. Wired.

Zollo, M., and Winter, S. G. (2002). Deliberate learning and the evolution of dynamic capabilities. Organization Science, 13(3), 339–351. https://doi.org/10.1287/orsc.13.3.339.2780

Zucker, L.G., 1987. Institutional theories of organization. *Annual review of sociology*, *13*(1), pp.443-464.

Appendix 1: Research Invite Letter (through LinkedIn InMail)

Hi

Hope you are keeping safe and well!

I am a bursary-holding doctoral researcher in corporate governance at the Henley Business school, University of Reading, conducting research through online (45-60 mins) elite interviews with UK-based board members of companies, who are associated with strategic decisions on technology cybersecurity.

I was referred to you by and would be obliged if you would be able to spare some time for me. While you must mostly associate with other business leaders, your views and experiences would be precious information for a researcher like me. I must mention that I am not requesting for any classified information from your end, and any/all information you share would be kept confidential.

If you could share your email id, I would share more information with you such as the purpose of the interview, information on its use, and management of data. My research has been approved from the University of Reading's Research Ethics Committee and I am in the early phases of my study.

I would be obliged to have your perspective and insights through this conversation.

Thank you.

Warmest wishes,

Ruchi Goyal

Doctoral Researcher | Marketing & Reputation Representative
Henley Business School | University of Reading
https://www.henley.ac.uk/people/person/ruchi-goyal
https://www.linkedin.com/in/ruchi-g-a009088/

Appendix 2: Interview Guide

The following broad themes guided the interview process, which were also influenced by inputs from previous participants' opinions and perspectives:

- Participant background and experience, relating to -
    - their involvement within their organisation and/or others they may be associated with (eg. Consultants, NEDs in other organisations, etc.)
    - the breadth and depth of their experience and involvement with cybersecurity decision-making
- Discussing leadership -
    - relationships between governing board and C-suite
    - nature of interactions between each side
    - demarcation of responsibilities
- Discussing Board of Directors -
    - with respect to the challenges of their role
    - contributions in their opinions made through their roles.
- Digitalisation and associated risks
    - with respect to legacy systems
    - levels of investment required in IT assets
    - adoption of emerging technologies
- Organisational strategy for cybersecurity
    - specific range of threats for their organisation
    - damage and/or impact from compromise caused by threats
    - protection planned and/or invested in

Appendix 3: Sample Interview Transcript